BULLETIN (SB21-214)

VULNERABILITY SUMMARY FOR THE WEEK OF

26TH JULY, 2021

Bulletin (SB21-214)
Vulnerability Summary for the Week of July 26, 2021

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
naviwebs -- navigatecms	In NavigateCMS version 2.9.4 and below, function in `product.php` is vulnerable to sql injection on parameter `products-order` through a post request, which results in arbitrary sql query execution in the backend database.	2021-07-26	7.5	CVE-2021-37473
naviwebs -- navigatecms	In NavigateCMS version 2.9.4 and below, function in `templates.php` is vulnerable to sql injection on parameter `template-properties-order`, which results in arbitrary sql query execution in the backend database.	2021-07-26	7.5	CVE-2021-37475
naviwebs -- navigatecms	In NavigateCMS version 2.9.4 and below, function in `product.php` is vulnerable to sql injection on parameter `id` through a post request, which results in arbitrary sql query execution in the backend database.	2021-07-26	7.5	CVE-2021-37476
naviwebs -- navigatecms	In NavigateCMS version 2.9.4 and below, function in `structure.php` is vulnerable to sql injection on parameter `children_order`, which results in arbitrary sql query execution in the backend database.	2021-07-26	7.5	CVE-2021-37477
sourcecodester -- e-commerce_website	Arbitrary file upload vulnerability in SourceCodester E-Commerce Website v 1.0 allows attackers to execute arbitrary code via the file upload to prodViewUpdate.php.	2021-07-23	7.5	CVE-2021-25207
sourcecodester -- responsive_ordering_system	Arbitrary file upload vulnerability in SourceCodester Responsive Ordering System v 1.0 allows attackers to execute arbitrary code via the file upload to Product_model.php.	2021-07-23	7.5	CVE-2021-25206
sourcecodester -- travel_management_system	Arbitrary file upload vulnerability in SourceCodester Travel Management System v 1.0 allows attackers to execute arbitrary code via the file upload to updatepackage.php.	2021-07-23	7.5	CVE-2021-25208
victor_cms_project -- victor_cms	Arbitrary file upload vulnerability in Victor CMS v 1.0 allows attackers to execute arbitrary code via the file upload to \CMSsite-master\admin\includes\admin_add_post.php.	2021-07-23	7.5	CVE-2021-25203
dlink -- dir-3040_firmware	A hard-coded password vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	7.5	CVE-2021-21820
microsoft -- malware_protection_engine	Microsoft Defender Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34522.	2021-07-16	9.3	CVE-2021-34464
microsoft -- windows_10	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34441, CVE-2021-34503.	2021-07-16	9.3	CVE-2021-34439
microsoft -- windows_10	Scripting Engine Memory Corruption Vulnerability	2021-07-16	9.3	CVE-2021-34448
microsoft -- windows_10	Windows Hyper-V Remote Code Execution Vulnerability	2021-07-16	9	CVE-2021-34450
microsoft -- windows_server_2016	Windows Kernel Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34508.	2021-07-16	9	CVE-2021-34458
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2456
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2463
oracle -- siebel_crm	Vulnerability in the Siebel CRM product of Oracle Siebel CRM (component: Siebel Core - Server Infrastructure). Supported versions that are affected are 21.5 and Prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Siebel CRM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	7.1	CVE-2021-2368

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2382
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	7.5	CVE-2021-2397
echobh -- sharecare	Echo ShareCare 8.15.5 is susceptible to SQL injection vulnerabilities when processing remote input from both authenticated and unauthenticated users, leading to the ability to bypass authentication, exfiltrate Structured Query Language (SQL) records, and manipulate data.	2021-07-13	7.5	CVE-2021-33578
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. It does not perform authentication or authorization checks when accessing a subset of sensitive resources, leading to the ability for unauthenticated users to access pages that are vulnerable to attacks such as SQL injection.	2021-07-13	7.5	CVE-2021-36124
espruino -- espruino	Buffer overflow vulnerability in function jsvGetStringChars in Espruino before RELEASE_2V09, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22884
fortinet -- forticlient	An improper symlink following in FortiClient for Mac 6.4.3 and below may allow an non-privileged user to execute arbitrary privileged shell commands during installation phase.	2021-07-12	7.2	CVE-2021-26089 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow an unauthenticated attacker to tamper with signed URLs by appending further data which allows bypass of signature verification.	2021-07-09	7.5	CVE-2021-24020 CONFIRM
fortinet -- fortimail	Multiple improper neutralization of special elements of SQL commands vulnerabilities in FortiMail before 6.4.4 may allow a non-authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	7.5	CVE-2021-24007 CONFIRM
golang -- go	golang/go in 1.0.2 fixes all.bash on shared machines. dotest() in src/pkg/debug/gosym/pclntab_test.go creates a temporary file with predicable name and executes it as shell script.	2021-07-09	7.5	CVE-2012-2666
google -- android	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181346550	2021-07-14	7.8	CVE-2021-0596
google -- android	In setNiNotification of GpsNetInitiatedHandler.java, there is a possible permissions bypass due to an empty mutable PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-154319182	2021-07-14	7.2	CVE-2020-0417
google -- android	In flv extractor, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187161771	2021-07-14	7.2	CVE-2021-0577
google -- android	In Factory::CreateStrictFunctionMap of factory.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-167389063	2021-07-14	10	CVE-2021-0515
google -- android	In beginWrite and beginRead of MessageQueueBase.h, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-184963385	2021-07-14	7.2	CVE-2021-0585

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onCreate of ConfirmConnectActivity, there is a possible remote bypass of user consent due to improper input validation. This could lead to remote (proximal, NFC) escalation of privilege allowing an attacker to deceive a user into allowing a Bluetooth connection with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176445224	2021-07-14	7.9	CVE-2021-0594
google -- android	In StreamOut::prepareForWriting of StreamOut.cpp, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-185259758	2021-07-14	7.2	CVE-2021-0587
google -- android	In BTM_TryAllocateSCN of btm_scn.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180939982	2021-07-14	7.2	CVE-2021-0589
google -- android	In various functions in WideVine, there are possible out of bounds writes due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-188061006	2021-07-14	9.3	CVE-2021-0592
google -- android	In several functions of the V8 library, there is a possible use after free due to a race condition. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9 Android-11 Android-8.1Android ID: A-162604069	2021-07-14	9.3	CVE-2021-0514
google -- android	In onCreateOptionsMenu of WifiNetworkDetailsFragment.java, there is a possible way for guest users to view and modify Wi-Fi settings for all configured APs due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-177573895	2021-07-14	7.2	CVE-2021-0602
halo -- halo	Remote Code Executon vulnerability in Halo 0.4.3 via the remoteAddr and themeName parameters.	2021-07-12	7.5	CVE-2020-18980
jsish -- jsish	Integer overflow vulnerability in function Jsi_ObjSetLength in jsish before 3.0.6, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22875
jsish -- jsish	Integer overflow vulnerability in function Jsi_ObjArraySizer in jsish before 3.0.8, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22874
jsish -- jsish	Buffer overflow vulnerability in function NumberToPrecisionCmd in jsish before 3.0.7, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22873
kaseya -- vsa	Kaseya VSA before 9.5.5 allows remote code execution.	2021-07-09	7.5	CVE-2021-30118
kramerav -- viaware	KramerAV VIAWare, all tested versions, allow privilege escalation through onfiguration of sudo. Sudoers permits running of multiple dangerous commands, including unzip, systemctl and dpkg.	2021-07-12	7.5	CVE-2021-35064
linux -- linux_kernel	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-07-09	7.2	CVE-2021-3612
linuxptp_project -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1.	2021-07-09	8	CVE-2021-3570 DEBIAN FEDORA FEDORA
metinfo -- metinfo	SQL Injection vulnerability in Metinfo 7.0.0beta in index.php.	2021-07-12	7.5	CVE-2020-21132
metinfo -- metinfo	SQL Injection vulnerability in Metinfo 7.0.0 beta in member/getpassword.php?lang=cn&a=dovalid.	2021-07-12	7.5	CVE-2020-21133
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-34473.	2021-07-14	7.5	CVE-2021-31206
microsoft -- windows_10	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31979, CVE-2021-34514.	2021-07-14	7.2	CVE-2021-33771
microsoft -- windows_10	Windows Security Account Manager Remote Protocol Security Feature Bypass Vulnerability	2021-07-14	7.5	CVE-2021-33757

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Secure Kernel Mode Security Feature Bypass Vulnerability	2021-07-14	7.2	CVE-2021-33744
microsoft -- windows_10	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33771, CVE-2021-34514.	2021-07-14	7.2	CVE-2021-31979
microsoft -- windows_10	Windows Media Remote Code Execution Vulnerability	2021-07-14	9.3	CVE-2021-33740
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server supports application specific tokens for authentication purposes. These tokens are supposed to be granted to a specific applications (e.g. DAV sync clients), and can also be configured by the user to not have any filesystem access. Due to a lacking permission check, the tokens were able to change their own permissions in versions prior to 19.0.13, 20.0.11, and 21.0.3. Thus fileystem limited tokens were able to grant themselves access to the filesystem. The issue is patched in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds aside from upgrading.	2021-07-12	7.5	CVE-2021-32688 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, webauthn tokens were not deleted after a user has been deleted. If a victim reused an earlier used username, the previous user could gain access to their account. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	7.5	CVE-2021-32726 CONFIRM
ninjateam -- filebird	The Filebird Plugin 4.7.3 introduced a SQL injection vulnerability as it is making SQL queries without escaping user input data from a HTTP post request. This is a major vulnerability as the user input is not escaped and passed directly to the get_col function and it allows SQL injection. The Rest API endpoint which invokes this function also does not have any required permissions/authentication and can be accessed by an anonymous user.	2021-07-12	7.5	CVE-2021-24385 CONFIRM
putil-merge_project -- putil-merge	Prototype pollution vulnerability in 'putil-merge' versions1.0.0 through 3.6.6 allows attacker to cause a denial of service and may lead to remote code execution.	2021-07-14	7.5	CVE-2021-25953
python -- pillow	Pillow through 8.2.0 and PIL (aka Python Imaging Library) through 1.1.7 allow an attacker to pass controlled parameters directly into a convert function to trigger a buffer overflow in Convert.c.	2021-07-13	7.5	CVE-2021-34552
qualcomm -- apq8009w_firmware	Buffer overflow in modem due to improper array index check before copying into it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	2021-07-13	10	CVE-2020-11307 CONFIRM
qualcomm -- apq8017_firmware	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1890 CONFIRM
qualcomm -- apq8017_firmware	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1886 CONFIRM
qualcomm -- apq8017_firmware	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1889 CONFIRM
qualcomm -- apq8017_firmware	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1888 CONFIRM
qualcomm -- aqt1000_firmware	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-07-13	7.2	CVE-2021-1931 CONFIRM
qualcomm -- aqt1000_firmware	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1940 CONFIRM
qualcomm -- aqt1000_firmware	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	10	CVE-2021-1965 CONFIRM
sap -- netweaver_as_abap	A function module of SAP NetWeaver AS ABAP (Reconciliation Framework), versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75C, 75D, 75E, 75F, allows a high privileged attacker to inject code that can be	2021-07-14	7.5	CVE-2021-33678

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	executed by the application. An attacker could thereby delete some critical information and could make the SAP system completely unavailable.			
solarwinds -- dameware_mini_remote_control	In SolarWinds DameWare Mini Remote Control Server 12.0.1.200, insecure file permissions allow file deletion as SYSTEM.	2021-07-13	9.4	CVE-2021-31217
totaljs -- total.js	The package total.js before 3.4.9 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.	2021-07-12	7.5	CVE-2021-23389
totaljs -- total4	The package total4 before 0.0.43 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.	2021-07-12	7.5	CVE-2021-23390
wms_project -- wms	SQL Injection in WMS v1.0 allows remote attackers to execute arbitrary code via the "username" parameter in the component "chkuser.php".	2021-07-12	7.5	CVE-2020-18544
wpdevart -- poll\,_survey\,_questionnaire_and_voting_system	The Poll, Survey, Questionnaire and Voting system WordPress plugin before 1.5.3 did not sanitise, escape or validate the date_answers[] POST parameter before using it in a SQL statement when sending a Poll result, allowing unauthenticated users to perform SQL Injection attacks	2021-07-12	7.5	CVE-2021-24442 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
learning_management_system_project -- learning_management_system	SQL injection vulnerability in Learning Management System v 1.0 allows remote attackers to execute arbitrary SQL statements through the id parameter to obtain sensitive database information.	2021-07-23	5	CVE-2021-25201
nchsoftware -- ivm_attendant	NCH IVM Attendant v5.12 and earlier suffers from a directory traversal weakness upon uploading plugins in a ZIP archive. This can lead to code execution if a ZIP element's pathname is set to a Windows startup folder, a file for the inbuilt Out-Going Message function, or a file for the the inbuilt Autodial function.	2021-07-25	6.5	CVE-2021-37444
nchsoftware -- ivm_attendant	NCH IVM Attendant v5.12 and earlier allows path traversal via the logdeleteselected check0 parameter for file deletion.	2021-07-25	5.5	CVE-2021-37443
nchsoftware -- ivm_attendant	NCH IVM Attendant v5.12 and earlier allows path traversal via viewfile?file=/.. to read files.	2021-07-25	4	CVE-2021-37442
nchsoftware -- quorum	In NCH Quorum v2.03 and earlier, an authenticated user can use directory traversal via logprop?file=/.. for file reading.	2021-07-25	4	CVE-2021-37445
omeka -- omeka	Cross Site Scripting (XSS) vulnerability in admin/files/edit in Omeka Classic <=2.7 allows remote attackers to inject arbitrary web script or HTML.	2021-07-23	4.3	CVE-2021-26799
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	4.3	CVE-2021-21803
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	4.3	CVE-2021-21802
advantech -- r-seenet	This vulnerability is present in device_graph_page.php script, which is a part of the Advantech R-SeeNet web applications. A specially crafted URL by an attacker and visited by a victim can lead to arbitrary JavaScript code execution.	2021-07-16	4.3	CVE-2021-21801
dlink -- dir-3040_firmware	A hard-coded password vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to a denial of service. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	5	CVE-2021-21818
dlink -- dir-3040_firmware	An information disclosure vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	5	CVE-2021-21817
dlink -- dir-3040_firmware	A code execution vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	2021-07-16	6.5	CVE-2021-21819
microsoft -- 365_apps	Microsoft Word Remote Code Execution Vulnerability	2021-07-16	6.8	CVE-2021-34452
microsoft -- office_online_server	Microsoft Office Online Server Spoofing Vulnerability	2021-07-16	5	CVE-2021-34451
microsoft -- sharepoint_foundation	Microsoft SharePoint Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34468, CVE-2021-34520.	2021-07-16	6.5	CVE-2021-34467
microsoft -- windows	Windows Print Spooler Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34481

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows MSHTML Platform Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34497.	2021-07-16	6.8	CVE-2021-34447
microsoft -- windows_10	Windows HTML Platforms Security Feature Bypass Vulnerability	2021-07-16	6.8	CVE-2021-34446
microsoft -- windows_10	Windows AppX Deployment Extensions Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34462
microsoft -- windows_10	Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34461
microsoft -- windows_10	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33751, CVE-2021-34510, CVE-2021-34512, CVE-2021-34513.	2021-07-16	4.6	CVE-2021-34460
microsoft -- windows_10	Microsoft Windows Media Foundation Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-34439, CVE-2021-34503.	2021-07-16	6.8	CVE-2021-34441
microsoft -- windows_10	Windows AppContainer Elevation Of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34459
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-33773, CVE-2021-34445.	2021-07-16	4.6	CVE-2021-34456
microsoft -- windows_10	Windows File History Service Elevation of Privilege Vulnerability	2021-07-16	4.6	CVE-2021-34455
microsoft -- windows_10	Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34516.	2021-07-16	4.6	CVE-2021-34449
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-33773, CVE-2021-34456.	2021-07-16	4.6	CVE-2021-34445
microsoft -- windows_10	Windows Font Driver Host Remote Code Execution Vulnerability	2021-07-16	6.8	CVE-2021-34438
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34442, CVE-2021-34499.	2021-07-16	4	CVE-2021-34444
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33745, CVE-2021-34444, CVE-2021-34499.	2021-07-16	5	CVE-2021-34442
mikrotik -- routeros	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the sshd process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	2021-07-19	4	CVE-2020-20230
mikrotik -- routeros	Mikrotik RouterOs before stable 6.47 suffers from an uncontrolled resource consumption in the memtest process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	2021-07-19	4	CVE-2020-20248
oracle -- access_manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Rest interfaces for Access Mgr). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	4	CVE-2021-2358

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- advanced_inbound_telephony	Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: SDK client integration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Inbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Inbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Inbound Telephony accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2361
oracle -- advanced_outbound_telephony	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Region Mapping). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Outbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2398
oracle -- application_express	Vulnerability in the Oracle Application Express Data Reporter component of Oracle Database Server. The supported version that is affected is Prior to 21.1.0.00.04. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Data Reporter. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Data Reporter, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Data Reporter accessible data as well as unauthorized read access to a subset of Oracle Application Express Data Reporter accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	4.9	CVE-2021-2460
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments / File Upload). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2021-07-21	4.9	CVE-2021-2380
oracle -- approvals_management	Vulnerability in the Oracle Approvals Management product of Oracle E-Business Suite (component: AME Page rendering). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Approvals Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Approvals Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Approvals Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2360

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	5	CVE-2021-2401
oracle -- bi_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	5	CVE-2021-2400
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	5	CVE-2021-2371
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	6.8	CVE-2021-2428
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	5	CVE-2021-2344
oracle -- collaborative_planning	Vulnerability in the Oracle Collaborative Planning product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Collaborative Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Collaborative Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Collaborative Planning accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2406
oracle -- commerce_experience_manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search /	2021-07-21	4.9	CVE-2021-2346

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle Commerce Experience Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).			
oracle -- commerce_experience_manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Tools and Frameworks). The supported version that is affected is 11.3.1.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	4.9	CVE-2021-2345
oracle -- commerce_service_center	Vulnerability in the Oracle Commerce Service Center product of Oracle Commerce (component: Commerce Service Center). Supported versions that are affected are 11.0.0, 11.1.0, 11.2.0 and 11.3.0-11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Service Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Service Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Service Center accessible data as well as unauthorized read access to a subset of Oracle Commerce Service Center accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	5.8	CVE-2021-2462
oracle -- core_rdbms	Vulnerability in the Core RDBMS component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows low privileged attacker having Create Table privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2021-07-21	4	CVE-2021-2330
oracle -- database	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Public Synonym privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in takeover of Oracle XML DB. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	6.5	CVE-2021-2337
oracle -- database_vault	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	4	CVE-2021-2326

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- engineering	Vulnerability in the Oracle Engineering product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Engineering. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Engineering accessible data as well as unauthorized access to critical data or complete access to all Oracle Engineering accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2405
oracle -- field_service	Vulnerability in the Oracle Field Service product of Oracle E-Business Suite (component: Wireless). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2362
oracle -- flexcube_universal_banking	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Loans And Deposits). Supported versions that are affected are 12.0-12.4, 14.0-14.4 and . Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N).	2021-07-21	4.9	CVE-2021-2324
oracle -- flexcube_universal_banking	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Flex-Branch). Supported versions that are affected are 12.3, 12.4, 14.0-14.4 and . Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	4.3	CVE-2021-2323
oracle -- graalvm	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	2021-07-21	4.3	CVE-2021-2341 CONFIRM
oracle -- graalvm	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Library). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with	2021-07-21	4.3	CVE-2021-2369 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).			
oracle -- hyperion_essbase_administration_services	Vulnerability in the Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Console). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. While the vulnerability is in Hyperion Essbase Administration Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2021-07-21	5	CVE-2021-2349
oracle -- hyperion_essbase_administration_services	Vulnerability in the Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Console). Supported versions that are affected are 11.1.2.4 and 21.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Essbase Administration Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	5	CVE-2021-2350
oracle -- hyperion_infrastructure_technology	Vulnerability in the Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:L/A:N).	2021-07-21	4.9	CVE-2021-2347
oracle -- identity_manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Request Management & Workflow). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Identity Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	5	CVE-2021-2457
oracle -- identity_manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Identity Console). Supported versions that are affected are 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Identity Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Identity Manager accessible data as well as unauthorized update, insert or delete access to some of	2021-07-21	4.9	CVE-2021-2458

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Identity Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).			
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.5.3 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	5.8	CVE-2021-2375
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime). Supported versions that are affected are 9.2.5.3 and Prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	4.9	CVE-2021-2373
oracle -- marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2021-07-21	5.8	CVE-2021-2359
oracle -- marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	6.4	CVE-2021-2355
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2021-07-21	4	CVE-2021-2340

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	6.8	CVE-2021-2339 CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H).	2021-07-21	4.9	CVE-2021-2356 CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	6.8	CVE-2021-2354 CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2357 CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	6.8	CVE-2021-2352 CONFIRM
oracle -- mysql_cluster	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: JS module). Supported versions that are affected are 8.0.25 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	2021-07-21	4.3	CVE-2021-2411 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2342

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2367 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2370 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2399 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2402 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	2021-07-21	4.9	CVE-2021-2385
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2412 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2422 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2424 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2425 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2426 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2427 CONFIRM
oracle -- mysql_server	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	4	CVE-2021-2410 CONFIRM
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2431

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2452
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2453
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2430
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2450

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2451
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2423
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N).	2021-07-21	5.8	CVE-2021-2449
oracle -- peoplesoft_enterprise_hcm_candidate_gateway	Vulnerability in the PeopleSoft Enterprise HCM Candidate Gateway product of Oracle PeopleSoft (component: e-mail notification). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Candidate Gateway. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Candidate Gateway accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Candidate Gateway accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2021-07-21	6.4	CVE-2021-2404
oracle -- peoplesoft_enterprise_hcm_shared_components	Vulnerability in the PeopleSoft Enterprise HCM Shared Components product of Oracle PeopleSoft (component: Person Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Shared	2021-07-21	5.5	CVE-2021-2455

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Components. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Shared Components accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Shared Components accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).			
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	5	CVE-2021-2407
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	4	CVE-2021-2377
oracle -- peoplesoft_enterprise_pt_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Notification Configuration). The supported version that is affected is 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	5.8	CVE-2021-2408
oracle -- public_sector_financials	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Public Sector Financials (International). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Public Sector Financials (International) accessible data as well as unauthorized access to critical data or complete access to all Oracle Public Sector Financials (International) accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2363
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2021-07-21	6.5	CVE-2021-2447

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- secure_global_desktop	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2021-07-21	6.8	CVE-2021-2446
oracle -- siebel_marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Email Marketing Stand-Alone). Supported versions that are affected are 21.5 and Prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Apps - Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Apps - Marketing accessible data as well as unauthorized read access to a subset of Siebel Apps - Marketing accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2021-07-21	5.8	CVE-2021-2338
oracle -- text	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Procedure, Alter Any Table privilege with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2021-07-21	6.5	CVE-2021-2328
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2021-07-21	4.6	CVE-2021-2409
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Solaris x86 and Linux systems only. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2021-07-21	4.6	CVE-2021-2443
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.24. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle	2021-07-21	4.4	CVE-2021-2454

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	VM VirtualBox. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).			
oracle -- web_applications_desktop_integrator	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Application Service). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Applications Desktop Integrator accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Applications Desktop Integrator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-07-21	5.5	CVE-2021-2434
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	5	CVE-2021-2376
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2021-07-21	5	CVE-2021-2378
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	5	CVE-2021-2403
oracle -- workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Workflow accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2021-07-21	4	CVE-2021-2343
oracle -- xml_database	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Alter User privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle XML DB accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2021-07-21	4	CVE-2021-2333
oracle -- xml_database	Vulnerability in the Oracle XML DB component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 19c. Easily	2021-07-21	6.5	CVE-2021-2329

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitable vulnerability allows high privileged attacker having Create Any Procedure, Create Public Synonym privilege with network access via Oracle Net to compromise Oracle XML DB. Successful attacks of this vulnerability can result in takeover of Oracle XML DB. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).			
apache -- ant	When reading a specially crafted TAR archive an Apache Ant build can be made to allocate large amounts of memory that finally leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	2021-07-14	4.3	CVE-2021-36373 MLIST MLIST MLIST
apache -- ant	When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amounts of memory that leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Commonly used derived formats from ZIP archives are for instance JAR files and many office files. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	2021-07-14	4.3	CVE-2021-36374 MLIST MLIST MLIST
apache -- tomcat	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.	2021-07-12	5	CVE-2021-33037
apache -- tomcat	A vulnerability in Apache Tomcat allows an attacker to remotely trigger a denial of service. An error introduced as part of a change to improve error handling during non-blocking I/O meant that the error flag associated with the Request object was not reset between requests. This meant that once a non-blocking I/O error occurred, all future requests handled by that request object would fail. Users were able to trigger non-blocking I/O errors, e.g. by dropping a connection, thereby creating the possibility of triggering a DoS. Applications that do not use non-blocking I/O are not exposed to this vulnerability. This issue affects Apache Tomcat 10.0.3 to 10.0.4; 9.0.44; 8.5.64.	2021-07-12	5	CVE-2021-30639 MLIST MLIST
artifex -- mujs	Buffer overflow vulnerability in function jsG_markobject in jsgc.c in mujs before 1.0.8, allows remote attackers to cause a denial of service.	2021-07-13	5	CVE-2020-22886
artifex -- mujs	Buffer overflow vulnerability in mujs before 1.0.8 due to recursion in the GC scanning phase, allows remote attackers to cause a denial of service.	2021-07-13	5	CVE-2020-22885
autodesk -- design_review	A maliciously crafted PDF, PICT or TIFF file can be used to write beyond the allocated buffer while parsing PDF, PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27036
autodesk -- design_review	A maliciously crafted TIFF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27039
autodesk -- design_review	A Type Confusion vulnerability in Autodesk 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. An attacker can leverage this to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27038
autodesk -- design_review	A maliciously crafted PNG, PDF or DWF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability can be exploited by remote attackers to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27037

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- design_review	A heap-based buffer overflow could occur while parsing PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27034
autodesk -- design_review	A maliciously crafted TIFF, PDF, PICT or DWF files in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PDF, PICT or DWF files. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27035
axiosys -- bento4	A buffer overflow vulnerability in Ap4ElstAtom.cpp of Bento 1.5.1-628 leads to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19719
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a direct copy to NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19722
axiosys -- bento4	An unhandled memory allocation failure in Core/AP4IkmsAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19720
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19718
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap48bdlAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19717
axiosys -- bento4	A heap buffer overflow vulnerability in Ap4TrunAtom.cpp of Bento 1.5.1-628 may lead to an out-of-bounds write while running mp42aac, leading to system crashes and a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19721
baidu -- umeditor	Cross Site Scripting (XSS) vulnerability in umeditor v1.2.3 via /public/common/umeditor/php/getcontent.php.	2021-07-14	4.3	CVE-2020-18145
bookingcore -- booking_core	The “Subscribe” feature in Ultimate Booking System Booking Core 1.7.0 is vulnerable to CSV formula injection. The input containing the excel formula is not being sanitized by the application. As a result when admin in backend download and open the csv, content of the cells are executed.	2021-07-14	6.8	CVE-2020-25445
bookingcore -- booking_core	Cross Site Request Forgery (CSRF) vulnerability in Booking Core - Ultimate Booking System Booking Core 1.7.0 . The CSRF token is not being validated when the request is sent as a GET method. This results in an unauthorized change in the user's email ID, which can later be used to reset the password. The new password will be sent to a modified email ID.	2021-07-14	4.3	CVE-2020-27379
brave -- brave	In Brave Desktop between versions 1.17 and 1.26.60, when adblocking is enabled and a proxy browser extension is installed, the CNAME adblocking feature issues DNS requests that used the system DNS settings instead of the extension's proxy settings, resulting in possible information disclosure.	2021-07-12	4.3	CVE-2021-22916
brave -- browser	Brave Browser Desktop between versions 1.17 and 1.20 is vulnerable to information disclosure by way of DNS requests in Tor windows not flowing through Tor if adblocking was enabled.	2021-07-12	4.3	CVE-2021-22917
codeblab -- glass	The Glass WordPress plugin through 1.3.2 does not sanitise or escape its "Glass Pages" setting before outputting in a page, leading to a Stored Cross-Site Scripting issue. Furthermore, the plugin did not have CSRF check in place when saving its settings, allowing the issue to be exploited via a CSRF attack.	2021-07-12	4.3	CVE-2021-24434 CONFIRM
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-07-12	4.6	CVE-2021-21590

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service user could potentially exploit this vulnerability to escalate privileges.	2021-07-12	4.6	CVE-2021-21589
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-07-12	4.6	CVE-2021-21591
dell -- powerflex_presentation_server	Dell EMC PowerFlex, v3.5.x contain a Cross-Site WebSocket Hijacking Vulnerability in the Presentation Server/WebUI. An unauthenticated attacker could potentially exploit this vulnerability by tricking the user into performing unwanted actions on the Presentation Server and perform which may lead to configuration changes.	2021-07-12	4.3	CVE-2021-21588
delta_project -- delta	dandavison delta before 0.8.3 on Windows resolves an executable's pathname as a relative path from the current directory.	2021-07-13	4.4	CVE-2021-36376 CONFIRM
devolutions -- devolutions_server	Devolutions Server before 2021.1.18, and LTS before 2020.3.20, allows attackers to intercept private keys via a man-in-the-middle attack against the connections/partial endpoint (which accepts cleartext).	2021-07-12	4.3	CVE-2021-36382
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The TextReader feature in General/TextReader/TextReader.cfm is susceptible to a local file inclusion vulnerability when processing remote input in the textFile parameter from an authenticated user, leading to the ability to read arbitrary files on the server filesystems as well any files accessible via Universal Naming Convention (UNC) paths.	2021-07-13	4	CVE-2021-36123
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The UnzipFile feature in Access/EligFeedParse_Sup/UnzipFile_Upd.cfm is susceptible to a command argument injection vulnerability when processing remote input in the zippass parameter from an authenticated user, leading to the ability to inject arbitrary arguments to 7z.exe.	2021-07-13	6.5	CVE-2021-36122
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The file-upload feature in Access/DownloadFeed_Mnt/FileUpload_Upd.cfm is susceptible to an unrestricted upload vulnerability via the name1 parameter, when processing remote input from an authenticated user, leading to the ability for arbitrary files to be written to arbitrary filesystem locations via ../ Directory Traversal on the Z: drive (a hard-coded drive letter where ShareCare application files reside) and remote code execution as the ShareCare service user (NT AUTHORITY\SYSTEM).	2021-07-13	6.5	CVE-2021-36121
edgexfoundry -- edgex_foundry	EdgeX Foundry is an open source project for building a common open framework for internet-of-things edge computing. A vulnerability exists in the Edinburgh, Fuji, Geneva, and Hanoi versions of the software. When the EdgeX API gateway is configured for OAuth2 authentication and a proxy user is created, the client_id and client_secret required to obtain an OAuth2 authentication token are set to the username of the proxy user. A remote network attacker can then perform a dictionary-based password attack on the OAuth2 token endpoint of the API gateway to obtain an OAuth2 authentication token and use that token to make authenticated calls to EdgeX microservices from an untrusted network. OAuth2 is the default authentication method in EdgeX Edinburgh release. The default authentication method was changed to JWT in Fuji and later releases. Users should upgrade to the EdgeX Ireland release to obtain the fix. The OAuth2 authentication method is disabled in Ireland release. If unable to upgrade and OAuth2 authentication is required, users should create OAuth2 users directly using the Kong admin API and forgo the use of the `security-proxy-setup` tool to create OAuth2 users.	2021-07-09	5.8	CVE-2021-32753 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
edifecs -- transaction_management	In Edifecs Transaction Management through 2021-07-12, an unauthenticated user can inject arbitrary text into a user's browser via logon.jsp?logon_error= on the login screen of the Web application.	2021-07-12	5	CVE-2021-36381
element-it -- http_commander	A Directory Traversal vulnerability in the Unzip feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to write files to arbitrary directories via relative paths in ZIP archives.	2021-07-14	4	CVE-2021-33211
element-it -- http_commander	An SSRF vulnerability in the "Upload from URL" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to retrieve HTTP and FTP files from the internal server network by inserting an internal address.	2021-07-14	4	CVE-2021-33213
esri -- arcgis_server	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-10	4.3	CVE-2021-29107 CONFIRM
esri -- arcgis_server	A reflected Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	2021-07-10	4.3	CVE-2021-29106 CONFIRM
esri -- arcgis_server	A Server-Side Request Forgery (SSRF) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote, unauthenticated attacker to forge GET requests to arbitrary URLs from the system, potentially leading to network enumeration or facilitating other attacks.	2021-07-11	6.4	CVE-2021-29102 CONFIRM
esri -- arcgis_server	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-11	4.3	CVE-2021-29104 CONFIRM
esri -- arcgis_server	A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	2021-07-11	4.3	CVE-2021-29103 CONFIRM
eventespresso -- event_espresso	A cross-site scripting (XSS) vulnerability in wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php in the Event Espresso Core plugin before 4.10.7.p for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2021-07-13	4.3	CVE-2020-26153
exiv2 -- exiv2	A buffer overflow vulnerability in the Databuf function in types.cpp of Exiv2 v0.27.1 leads to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19716
exiv2 -- exiv2	An integer overflow vulnerability in the getUShort function of Exiv2 0.27.1 results in segmentation faults within the application, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19715
fetchdesigns -- sign-up_sheets	The Sign-up Sheets WordPress plugin before 1.0.14 does not not sanitise or validate the Sheet title when generating the CSV to export, which could lead to a CSV injection issue	2021-07-12	6	CVE-2021-24441 CONFIRM
fortinet -- fortiap	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments.	2021-07-09	4.6	CVE-2021-26106 CONFIRM
fortinet -- fortimail	A missing release of memory after its effective lifetime vulnerability in the Webmail of FortiMail 6.4.0 through 6.4.4 and 6.2.0 through 6.2.6 may allow an unauthenticated remote attacker to exhaust available memory via specifically crafted login requests.	2021-07-12	5	CVE-2021-26090 CONFIRM
fortinet -- fortimail	An improper neutralization of special elements used in an OS Command vulnerability in the administrative interface of FortiMail before 6.4.4 may allow an	2021-07-12	6.5	CVE-2021-24015 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attacker to execute unauthorized commands via specifically crafted HTTP requests.			
fortinet -- fortimail	A missing cryptographic step in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an unauthenticated attacker who intercepts the encrypted messages to manipulate them in such a way that makes the tampering and the recovery of the plaintexts possible.	2021-07-09	5	CVE-2021-26100 CONFIRM
fortinet -- fortimail	Multiple Path traversal vulnerabilities in the Webmail of FortiMail before 6.4.4 may allow a regular user to obtain unauthorized access to files and data via specifically crafted web requests.	2021-07-12	4	CVE-2021-24013 CONFIRM
fortinet -- fortimail	Missing cryptographic steps in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an attacker who comes in possession of the encrypted master keys to compromise their confidentiality by observing a few invariant properties of the ciphertext.	2021-07-12	4	CVE-2021-26099 CONFIRM
fortinet -- fortimail	Multiple instances of incorrect calculation of buffer size in the Webmail and Administrative interface of FortiMail before 6.4.5 may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	6.5	CVE-2021-22129 CONFIRM
fortinet -- fortisandbox	A concurrent execution using shared resource with improper synchronization ('race condition') in the command shell of FortiSandbox before 3.2.2 may allow an authenticated attacker to bring the system into an unresponsive state via specifically orchestrated sequences of commands.	2021-07-09	6.3	CVE-2020-29014 CONFIRM
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled.	2021-07-09	4.3	CVE-2021-33795
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary.	2021-07-09	6.8	CVE-2021-33792
getambassador -- emissary-ingress	Emissary-Ingress (formerly Ambassador API Gateway) through 1.13.9 allows attackers to bypass client certificate requirements (i.e., mTLS cert_required) on backend upstreams when more than one TLSContext is defined and at least one configuration exists that does not require client certificate authentication. The attacker must send an SNI specifying an unprotected backend and an HTTP Host header specifying a protected backend. (2.x versions are unaffected. 1.x versions are unaffected with certain configuration settings involving prune_unreachable_routes and a wildcard Host resource.)	2021-07-09	4.3	CVE-2021-36371
google -- android	In handleSendStatusChangeBroadcast of WifiDisplayAdapter.java, there is a possible leak of location-sensitive data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176541017	2021-07-14	4.9	CVE-2021-0518
google -- android	In onCreate of DevicePickerFragment.java, there is a possible way to trick the user to select an unwanted bluetooth device due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-182584940	2021-07-14	6.9	CVE-2021-0586
google -- android	In processInboundMessage of MceStateMachine.java, there is a possible SMS disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-177238342	2021-07-14	4.9	CVE-2021-0588
google -- android	In onCreate of PermissionActivity.java, there is a possible permission bypass due to Confusing UI. This could lead to local escalation of privilege with no additional	2021-07-14	4.4	CVE-2021-0441

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174495520			
google -- android	In onCreate of DeviceAdminAdd.java, there is a possible way to mislead a user to activate a device admin app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-179042963	2021-07-14	6.9	CVE-2021-0600
google -- android	In encodeFrames of avc_enc_fuzzer.cpp, there is a possible out of bounds write due to a double free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-180643802	2021-07-14	4.9	CVE-2021-0601
google -- android	In onCreate of ContactSelectionActivity.java, there is a possible way to get access to contacts without permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-182809425	2021-07-14	4.4	CVE-2021-0603
google -- android	In sendNetworkConditionsBroadcast of NetworkMonitor.java, there is a possible way for a privileged app to receive WiFi BSSID and SSID without location permissions due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-175213041	2021-07-14	4.9	CVE-2021-0590
google -- android	In onPackageAddedInternal of PermissionManagerService.java, there is possible access to external storage due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-171430330	2021-07-14	4.6	CVE-2021-0486
google -- android	In scheduleTimeoutLocked of NotificationRecord.java, there is a possible disclosure of a sensitive identifier via broadcasted intent due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175614289	2021-07-14	4.9	CVE-2021-0599
google -- android	In notifyProfileAdded and notifyProfileRemoved of SipService.java, there is a possible way to retrieve SIP account names due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176496502	2021-07-14	4.9	CVE-2021-0597
halo -- halo	File Deletion vulnerability in Halo 0.4.3 via delBackup.	2021-07-12	6.4	CVE-2020-19038
halo -- halo	Incorrect Access Control vulnearbility in Halo 0.4.3, which allows a malicious user to bypass encrption to view encrpted articles via cookies.	2021-07-12	5	CVE-2020-19037
halo -- halo	Cross Siste Scripting (XSS) vulnerablity in Halo 0.4.3 via the X-forwarded-for Header parameter.	2021-07-12	4.3	CVE-2020-18979
halo -- halo	SSRF vulnerability in Halo <=1.3.2 exists in the SMTP configuration, which can detect the server intranet.	2021-07-12	5	CVE-2020-23079
hms-networks -- ecatcher	In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.	2021-07-09	6	CVE-2021-33214

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hmtalk -- daviewindy	DaviewIndy v8.98.7.0 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed format file that is mishandled by DaviewIndy. Attackers could exploit this and arbitrary code execution.	2021-07-12	6.8	CVE-2020-7872
huawei -- harmonyos	A component of the HarmonyOS 2.0 has a Null Pointer Dereference Vulnerability. Local attackers may exploit this vulnerability to cause system denial of service.	2021-07-14	4.9	CVE-2021-22318
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could allow an authenticated user gain escalated privilesges due to improper application permissions. IBM X-Force ID: 196308.	2021-07-13	6.5	CVE-2021-20423 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could disclose sensitive information to a malicious attacker by accessing data stored in memory. IBM X-Force ID: 196304.	2021-07-13	5	CVE-2021-20422 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195361.	2021-07-13	4.3	CVE-2021-20369 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195031.	2021-07-13	5	CVE-2021-20360 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. X-Force ID: 196309.	2021-07-13	4	CVE-2021-20424 XF CONFIRM
ibm -- event_streams	IBM Event Streams 10.0, 10.1, 10.2, and 10.3 could allow a user the CA private key to create their own certificates and deploy them in the cluster and gain privileges of another user. IBM X-Force ID: 203450.	2021-07-12	6.5	CVE-2021-29792 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.2 could allow a user to bruce force sensitive information due to not properly limiting the number of interactions. IBM X-Force ID: 196216.	2021-07-12	4	CVE-2021-20414 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 200966.	2021-07-09	4.3	CVE-2021-29712 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 201164.	2021-07-09	6.5	CVE-2021-29730 XF CONFIRM
ibm -- mq_appliance	IBM MQ Appliance 9.1 and 9.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 191815.	2021-07-12	6.8	CVE-2020-4938 CONFIRM XF
ibm -- tivoli_netcool\/impact	IBM Tivoli Netcool/Impact 7.1.0.20 and 7.1.0.21 uses an insecure SSH server configuration which enables weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 203556.	2021-07-12	5	CVE-2021-29794 XF CONFIRM
icinga -- icinga	Icinga Web 2 is an open source monitoring web interface, framework, and command-line interface. A vulnerability in which custom variables are exposed to unauthorized users exists between versions 2.0.0 and 2.8.2. Custom variables are user-defined keys and values on configuration objects in Icinga 2. These are commonly used to reference secrets in other configurations such as check commands to be able to authenticate with a service being checked. Icinga Web 2 displays these custom variables to logged in users with access to said hosts or services. In order to protect the secrets from being visible to anyone, it's possible	2021-07-12	4	CVE-2021-32747 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to setup protection rules and blacklists in a user's role. Protection rules result in `***` being shown instead of the original value, the key will remain. Backlists will hide a custom variable entirely from the user. Besides using the UI, custom variables can also be accessed differently by using an undocumented URL parameter. By adding a parameter to the affected routes, Icinga Web 2 will show these columns additionally in the respective list. This parameter is also respected when exporting to JSON or CSV. Protection rules and blacklists however have no effect in this case. Custom variables are shown as-is in the result. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, one may set up a restriction to hide hosts and services with the custom variable in question.			
ipfire -- ipfire	Lightning Wire Labs IPFire 2.21 (x86_64) - Core Update 130 is affected by: Cross Site Scripting (XSS). The impact is: Session Hijacking (local). The component is: Affected at Routing configuration via the "Remark" text box or "remark" parameter. The attack vector is: Attacker need to craft the malicious javascript code.	2021-07-12	4.3	CVE-2020-19204
jsish -- jsish	Stack overflow vulnerability in function jsi_evalcode_sub in jsish before 3.0.18, allows remote attackers to cause a Denial of Service via a crafted value to the execute parameter.	2021-07-13	5	CVE-2020-22907
kaseya -- vsa	SQL injection exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30117
kaseya -- vsa	Local file inclusion exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30121
kaseya -- vsa	Kaseya VSA through 9.5.7 allows attackers to bypass the 2FA requirement.	2021-07-09	5	CVE-2021-30120
kaseya -- vsa	An XML External Entity (XXE) issue exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30201
linecorp -- line	LINE client for iOS before 10.16.3 allows cross site script with specific header in WebView.	2021-07-13	4.3	CVE-2021-36214
linuxfoundation -- grpc_swift	Mismanaged state in GRPCWebToHTTP2ServerCodec.swift in gRPC Swift 1.1.0 and 1.1.1 allows remote attackers to deny service by sending malformed requests.	2021-07-09	5	CVE-2021-36153
linuxfoundation -- grpc_swift	LengthPrefixedMessageReader in gRPC Swift 1.1.0 and earlier allocates buffers of arbitrary length, which allows remote attackers to cause uncontrolled resource consumption and deny service.	2021-07-09	5	CVE-2021-36155
linuxfoundation -- grpc_swift	HTTP2ToRawGRPCServerCodec in gRPC Swift 1.1.1 and earlier allows remote attackers to deny service via the delivery of many small messages within a single HTTP/2 frame, leading to Uncontrolled Recursion and stack consumption.	2021-07-09	5	CVE-2021-36154
linuxptp_project -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1.	2021-07-09	5.5	CVE-2021-3571 FEDORA FEDORA
metinfo -- metinfo	SQL Injection vulnerability in MetInfo 7.0.0beta via admin/?n=language&c=language_web&a=doAddLanguage.	2021-07-12	6.5	CVE-2020-21131
microfocus -- netiq_advanced_authentication	Multi-Factor Authentication (MFA) functionality can be bypassed, allowing the use of single factor authentication in NetIQ Advanced Authentication versions prior to 6.3 SP4 Patch 1.	2021-07-12	4	CVE-2021-22515 CONFIRM
microsoft -- bing	Microsoft Bing Search Spoofing Vulnerability	2021-07-14	4.3	CVE-2021-33753
microsoft -- exchange_server	Microsoft Exchange Information Disclosure Vulnerability	2021-07-14	5	CVE-2021-33766

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31206, CVE-2021-34473.	2021-07-14	6.5	CVE-2021-31196
microsoft -- exchange_server	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34470, CVE-2021-34523.	2021-07-14	5.2	CVE-2021-33768
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33776, CVE-2021-33777.	2021-07-14	6.8	CVE-2021-33778
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33776, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33775
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33776
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33776, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33777
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33775, CVE-2021-33776, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-31947
microsoft -- open_enclave_software_development_kit	Open Enclave SDK Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33767
microsoft -- power_bi_report_server	Power BI Remote Code Execution Vulnerability	2021-07-14	6.8	CVE-2021-31984
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33773, CVE-2021-34445, CVE-2021-34456.	2021-07-14	4.6	CVE-2021-33761
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33772, CVE-2021-34490.	2021-07-14	5	CVE-2021-31183
microsoft -- windows_10	Windows Desktop Bridge Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33759
microsoft -- windows_10	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34460, CVE-2021-34510, CVE-2021-34512, CVE-2021-34513.	2021-07-14	4.6	CVE-2021-33751
microsoft -- windows_10	Windows Projected File System Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33743
microsoft -- windows_10	Windows Event Tracing Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33774
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-34445, CVE-2021-34456.	2021-07-14	4.6	CVE-2021-33773
microsoft -- windows_10	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33784
microsoft -- windows_10	Windows Authenticode Spoofing Vulnerability	2021-07-14	4.3	CVE-2021-33782

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33750, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33752
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33755.	2021-07-14	4	CVE-2021-33758
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-31183, CVE-2021-34490.	2021-07-14	5	CVE-2021-33772
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33750, CVE-2021-33752.	2021-07-14	6.8	CVE-2021-33756
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33758.	2021-07-14	5	CVE-2021-33755
microsoft -- windows_10	Windows SMB Information Disclosure Vulnerability	2021-07-14	4	CVE-2021-33783
microsoft -- windows_10	Windows AF_UNIX Socket Provider Denial of Service Vulnerability	2021-07-14	5	CVE-2021-33785
microsoft -- windows_10	Azure AD Security Feature Bypass Vulnerability	2021-07-14	5.5	CVE-2021-33781
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33750, CVE-2021-33752, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33749
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33752, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33750
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33754, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6.5	CVE-2021-33780
microsoft -- windows_server_2008	Windows Key Distribution Center Information Disclosure Vulnerability	2021-07-14	4.3	CVE-2021-33764
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33754, CVE-2021-33780, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6.5	CVE-2021-33746
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-34442, CVE-2021-34444, CVE-2021-34499.	2021-07-14	4	CVE-2021-33745
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33780, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6	CVE-2021-33754
microsoft -- windows_server_2016	Windows ADFS Security Feature Bypass Vulnerability	2021-07-14	5.5	CVE-2021-33779
mikrotik -- routeros	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). NOTE: this is different from CVE-2020-20253 and CVE-2020-20254. All four vulnerabilities in the /nova/bin/lcdstat process are discussed in the CVE-2020-20250 github.com/cq674350529 reference.	2021-07-13	4	CVE-2020-20250

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mikrotik -- routeros	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-07-13	4	CVE-2020-20252
mitre -- caldera	A command injection vulnerability in the sandcat plugin of Caldera 2.3.1 and earlier allows authenticated attackers to execute any command or service.	2021-07-12	6.5	CVE-2020-19907
moddable -- moddable	Issue was discovered in the fxParserTree function in moddable, allows attackers to cause denial of service via a crafted payload. Fixed in commit 723816ab9b52f807180c99fc69c7d08cf6c6bd61.	2021-07-13	5	CVE-2020-22882
nextcloud -- nextcloud	Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.16.1, the Nextcloud Android client skipped a step that involved the client checking if a private key belonged to a previously downloaded public certificate. If the Nextcloud instance served a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. The vulnerability is patched in version 3.16.1. As a workaround, do not add additional end-to-end encrypted devices to a user account.	2021-07-12	5	CVE-2021-32727 CONFIRM
nextcloud -- nextcloud_mail	Nextcloud Mail is a mail app for Nextcloud. In versions prior to 1.9.6, the Nextcloud Mail application does not, by default, render images in emails to not leak the read state. The privacy filter failed to filter images with a `background-image` CSS attribute. Note that the images were still passed through the Nextcloud image proxy, and thus there was no IP leakage. The issue was patched in version 1.9.6 and 1.10.0. No workarounds are known to exist.	2021-07-12	4	CVE-2021-32707 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site scripting vulnerability is present in versions prior to 19.0.13, 20.0.11, and 21.0.3. The Nextcloud Text application shipped with Nextcloud server used a `text/html` Content-Type when serving files to users. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, use a browser that has support for Content-Security-Policy.	2021-07-12	4.3	CVE-2021-32733 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the shareinfo endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32703 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public DAV endpoint. This may have allowed an attacker to enumerate potentially valid share tokens or credentials. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32705 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, filenames where not escaped by default in controllers using `DownloadResponse`. When a user-supplied filename was passed unsanitized into a `DownloadResponse`, this could be used to trick users into downloading malicious files with a benign file extension. This would show in UI behaviours where Nextcloud applications would display a benign file extension (e.g. JPEG), but the file will actually be downloaded with an executable file extension. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. Administrators of Nextcloud instances do not have a workaround available, but developers of Nextcloud apps may manually escape the file name before passing it into `DownloadResponse`.	2021-07-12	6.8	CVE-2021-32679 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, ratelimits are not applied to OCS API responses. This affects any OCS API controller (`OCSController`) using the `@BruteForceProtection` annotation. Risk depends on the installed applications on the Nextcloud Server, but could range from bypassing authentication ratelimits or spamming other Nextcloud users. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. No workarounds aside from upgrading are known to exist.	2021-07-12	5	CVE-2021-32678 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public share link mount endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32741 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, the Nextcloud Text application shipped with Nextcloud Server returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, one may disable the Nextcloud Text application in Nextcloud Server app settings.	2021-07-12	5	CVE-2021-32734 CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, default share permissions were not being respected for federated reshares of files and folders. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32725 CONFIRM
nextcloud -- talk	Nextcloud Talk is a fully on-premises audio/video and chat communication service. In versions prior to 11.2.2, if a user was able to reuse an earlier used username, they could get access to any chat message sent to the previous user with this username. The issue was patched in versions 11.2.2 and 11.3.0. As a workaround, don't allow users to choose usernames themselves. This is the default behaviour of Nextcloud, but some user providers may allow doing so.	2021-07-12	4	CVE-2021-32689 CONFIRM
nodejs -- node.js	Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when uv__idna_toascii() is used to convert strings to ASCII. The pointer p is read and increased without checking whether it is beyond pe, with the latter holding a pointer to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via uv_getaddrinfo().	2021-07-12	6.4	CVE-2021-22918
nodejs -- node.js	Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking.	2021-07-12	4.4	CVE-2021-22921
openvpn -- openvpn	OpenVPN 3 Core Library version 3.6 and 3.6.1 allows a man-in-the-middle attacker to bypass the certificate authentication by issuing an unrelated server certificate using the same hostname found in the verify-x509-name option in a client configuration.	2021-07-12	5.8	CVE-2021-3547
panasonic -- fpwin_pro	Panasonic FPWIN Pro, all Versions 7.5.1.1 and prior, allows an attacker to craft a project file specifying a URI that causes the XML parser to access the URI and embed the contents, which may allow the attacker to disclose information that is accessible in the context of the user executing software.	2021-07-09	4.3	CVE-2021-32972
pbootcms -- pbootcms	Incorrect Access Control vulnerability in PbootCMS 2.0.6 via the list parameter in the update function in upgradecontroller.php.	2021-07-09	4	CVE-2020-22535
pfsense -- pfsense	Netgate pfSense Community Edition 2.4.4 - p2 (arm64) is affected by: Cross Site Scripting (XSS). The impact is: Session Hijacking, Information Leakage (local). The	2021-07-12	4.3	CVE-2020-19203

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	component is: pfSense Dashboard, Work-on-LAN Service configuration. The attack vector is: Inject the malicious JavaScript code in Description text box or parameter.			
plugin-planet -- prismatic	The Prismatic WordPress plugin before 2.8 does not escape the 'tab' GET parameter before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue which will be executed in the context of a logged in administrator	2021-07-12	4.3	CVE-2021-24409 CONFIRM
pluginus -- wordpress_meta_data_and_taxonomies_filter	Cross-site request forgery (CSRF) vulnerability in WordPress Meta Data Filter & Taxonomies Filter versions prior to v.1.2.8 and versions prior to v.2.2.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-14	6.8	CVE-2021-20781
putty -- putty	PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user).	2021-07-09	5.8	CVE-2021-36367
qualcomm -- apq8009_firmware	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	5	CVE-2021-1955 CONFIRM
qualcomm -- apq8053_firmware	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-07-13	5	CVE-2021-1970 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-07-13	5	CVE-2021-1907 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1964 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1943 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1954 CONFIRM
qualcomm -- apq8053_firmware	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1945 CONFIRM
qualcomm -- aqt1000_firmware	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1953 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- aqt1000_firmware	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1938 CONFIRM
qualcomm -- ar7420_firmware	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1887 CONFIRM
quickjs_project -- quickjs	Buffer Overflow vulnerability in quickjs.c in QuickJS, allows remote attackers to cause denial of service. This issue is resolved in the 2020-07-05 release.	2021-07-13	5	CVE-2020-22876
redhat -- keycloak	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.	2021-07-09	5	CVE-2021-3637
restsharp -- restsharp	RestSharp < 106.11.8-alpha.0.13 uses a regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS) when converting strings into DateTimes. If a server responds with a malicious string, the client using RestSharp will be stuck processing it for an exceedingly long time. Thus the remote server can trigger Denial of Service.	2021-07-12	5	CVE-2021-27293
retty -- retty	Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	2021-07-14	5	CVE-2021-20748
retty -- retty	Improper authorization in handler for custom URL scheme vulnerability in Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	2021-07-14	4.3	CVE-2021-20747
rockwellautomation -- micrologix_1100_firmware	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode.	2021-07-09	5	CVE-2021-33012
salonbookingsystem -- salon_booking_system	The Salon booking system WordPress plugin before 6.3.1 does not properly sanitise and escape the First Name field when booking an appointment, allowing low privilege users such as subscriber to set JavaScript in them, leading to a Stored Cross-Site Scripting (XSS) vulnerability. The Payload will then be triggered when an admin visits the "Calendar" page and the malicious script is executed in the admin context.	2021-07-12	4.3	CVE-2021-24429 CONFIRM
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes out of bounds write and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	2021-07-14	4.3	CVE-2021-33681
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes buffer overflow and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	2021-07-14	4.3	CVE-2021-33680
sap -- businessobjects_web_intelligence	Under certain conditions, SAP Business Objects Web Intelligence (BI Launchpad) versions - 420, 430, allows an attacker to access jsp source code, through SDK calls, of Analytical Reporting bundle, a part of the frontend application, which would otherwise be restricted.	2021-07-14	4	CVE-2021-33667

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- customer_relationship_management	A missing authority check in SAP CRM, versions - 700, 701, 702, 712, 713, 714, could be leveraged by an attacker with high privileges to compromise confidentiality, integrity, or availability of the system.	2021-07-14	6.5	CVE-2021-33676
sap -- netweaver_abap	SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 702, 730, 731, 804, 740, 750, 784, expose functions to external which can lead to information disclosure.	2021-07-14	5	CVE-2021-33677
sap -- netweaver_application_server_java	When user with insufficient privileges tries to access any application in SAP NetWeaver Administrator (Administrator applications), version - 7.50, no security audit log is created. Therefore, security audit log Integrity is impacted.	2021-07-14	4	CVE-2021-33689
sap -- netweaver_application_server_java	SAP NetWeaver AS for Java (Http Service Monitoring Filter), versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send multiple HTTP requests with different method types thereby crashing the filter and making the HTTP server unavailable to other legitimate users leading to denial of service vulnerability.	2021-07-14	5	CVE-2021-33670
sap -- netweaver_application_server_java	SAP NetWeaver AS JAVA (Enterprise Portal), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50 reveals sensitive information in one of their HTTP requests, an attacker can use this in conjunction with other attacks such as XSS to steal this information.	2021-07-14	4	CVE-2021-33687
sap -- netweaver_guided_procedures	SAP NetWeaver Guided Procedures (Administration Workset), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. The impact of missing authorization could result to abuse of functionality restricted to a particular user group, and could allow unauthorized users to read, modify or delete restricted data.	2021-07-14	6.5	CVE-2021-33671
segment -- is-email	A ReDoS (regular expression denial of service) flaw was found in the Segment is-email package before 1.0.1 for Node.js. An attacker that is able to provide crafted input to the isEmail(input) function may cause an application to consume an excessive amount of CPU.	2021-07-14	5	CVE-2021-36716 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13404)	2021-07-13	6.8	CVE-2021-34319 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13442)	2021-07-13	6.8	CVE-2021-34331 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13430)	2021-07-13	6.8	CVE-2021-34330 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427)	2021-07-13	6.8	CVE-2021-34329 CONFIRM CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13199)	2021-07-13	4.3	CVE-2021-34304 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422)	2021-07-13	6.8	CVE-2021-34326 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13420)	2021-07-13	6.8	CVE-2021-34324 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13419)	2021-07-13	6.8	CVE-2021-34323 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The DL180CoolType.dll library in affected applications lacks proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13380)	2021-07-13	6.8	CVE-2021-34316 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423)	2021-07-13	6.8	CVE-2021-34327 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13343)	2021-07-13	4.3	CVE-2021-34307 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13356)	2021-07-13	6.8	CVE-2021-34315 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files.	2021-07-13	6.8	CVE-2021-34314 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13355)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13354)	2021-07-13	6.8	CVE-2021-34313 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13353)	2021-07-13	6.8	CVE-2021-34312 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Mono_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13352)	2021-07-13	6.8	CVE-2021-34311 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13192)	2021-07-13	4.3	CVE-2021-34299 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13197)	2021-07-13	4.3	CVE-2021-34302 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13198)	2021-07-13	4.3	CVE-2021-34303 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13403)	2021-07-13	6.8	CVE-2021-34318 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424)	2021-07-13	6.8	CVE-2021-34328 CONFIRM CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCX files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13402)	2021-07-13	6.8	CVE-2021-34317 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12956)	2021-07-13	6.8	CVE-2021-34291 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13057)	2021-07-13	6.8	CVE-2021-34296 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12959)	2021-07-13	6.8	CVE-2021-34292 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The VisDraw.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13414)	2021-07-13	4.3	CVE-2021-34321 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13406)	2021-07-13	4.3	CVE-2021-34320 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13421)	2021-07-13	4.3	CVE-2021-34325 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in an infinite loop condition that leads to denial of service condition. An attacker could leverage this vulnerability to consume excessive resources. (CNVD-C-2021-79300)	2021-07-13	4.3	CVE-2021-34332 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in double free of an allocated buffer that leads	2021-07-13	4.3	CVE-2021-34333 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to a crash. An attacker could leverage this vulnerability to cause denial of service condition. (CNVD-C-2021-79295)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13351)	2021-07-13	6.8	CVE-2021-34310 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13344)	2021-07-13	4.3	CVE-2021-34308 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The JPEG2K_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13416)	2021-07-13	4.3	CVE-2021-34322 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13350)	2021-07-13	6.8	CVE-2021-34309 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13024)	2021-07-13	6.8	CVE-2021-34295 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13342)	2021-07-13	6.8	CVE-2021-34306 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13340)	2021-07-13	6.8	CVE-2021-34305 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13020)	2021-07-13	6.8	CVE-2021-34293 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing	2021-07-13	6.8	CVE-2021-34301 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13196)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13194)	2021-07-13	6.8	CVE-2021-34300 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13060)	2021-07-13	6.8	CVE-2021-34298 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13023	2021-07-13	6.8	CVE-2021-34294 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13059)	2021-07-13	6.8	CVE-2021-34297 CONFIRM
sonicwall -- switch	Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an attacker to cause a system instability or potentially read sensitive information from the memory locations.	2021-07-09	6.8	CVE-2021-20024 CONFIRM
stormshield -- endpoint_security	Stormshield Endpoint Security Evolution 2.0.0 through 2.0.2 does not accomplish the intended defense against local administrators who can replace the Visual C++ runtime DLLs (in %WINDIR%\system32) with malicious ones.	2021-07-13	4.6	CVE-2021-35957
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows deleting some resources not currently in use by any security policy by leveraging access to a computer having the administration console installed.	2021-07-13	4.3	CVE-2021-31225
tipsandtricks-hq -- software_license_manager	Cross-site request forgery (CSRF) vulnerability in Software License Manager versions prior to 4.4.6 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-14	6.8	CVE-2021-20782
vmware -- cloud_foundation	SFCB (Small Footprint CIM Broker) as used in ESXi has an authentication bypass vulnerability. A malicious actor with network access to port 5989 on ESXi may exploit this issue to bypass SFCB authentication by sending a specially crafted request.	2021-07-13	6.8	CVE-2021-21994
vmware -- cloud_foundation	OpenSLP as used in ESXi has a denial-of-service vulnerability due a heap out-of-bounds read issue. A malicious actor with network access to port 427 on ESXi may be able to trigger a heap out-of-bounds read in OpenSLP service resulting in a denial-of-service condition.	2021-07-13	5	CVE-2021-21995
vmware -- thinapp	VMware Thinapp version 5.x prior to 5.2.10 contain a DLL hijacking vulnerability due to insecure loading of DLLs. A malicious actor with non-administrative privileges may exploit this vulnerability to elevate privileges to administrator level on the Windows operating system having VMware ThinApp installed on it.	2021-07-13	6.9	CVE-2021-22000 FULLDISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
voidtools -- everything	HTTP header injection vulnerability in Everything all versions except the Lite version may allow a remote attacker to inject an arbitrary script or alter the website that uses the product via unspecified vectors.	2021-07-14	5.8	CVE-2021-20784
wayang-cms_project -- wayang-cms	A SQL injection vulnerability in wy_controlls/wy_side_visitor.php of Wayang-CMS v1.0 allows attackers to obtain sensitive database information.	2021-07-14	5	CVE-2020-29147
wayang-cms_project -- wayang-cms	A cross site scripting (XSS) vulnerability in index.php of Wayang-CMS v1.0 allows attackers to execute arbitrary web scripts or HTML via a constructed payload created by adding the X-Forwarded-For field to the header.	2021-07-14	4.3	CVE-2020-29146
wire -- wire	Wire is a collaboration platform. wire-ios-transport handles authentication of requests, network failures, and retries for the iOS implementation of Wire. In the 3.82 version of the iOS application, a new web socket implementation was introduced for users running iOS 13 or higher. This new websocket implementation is not configured to enforce certificate pinning when available. Certificate pinning for the new websocket is enforced in version 3.84 or above.	2021-07-13	4	CVE-2021-32755 CONFIRM
xen-orchestra -- xo-server	Xen Orchestra (with xo-web through 5.80.0 and xo-server through 5.84.0) mishandles authorization, as demonstrated by modified WebSocket resourceSet.getAll data is which the attacker changes the permission field from none to admin. The attacker gains access to data sets such as VMs, Backups, Audit, Users, and Groups.	2021-07-12	4	CVE-2021-36383
xml\ -- \	It was discovered that the XML::Atom Perl module before version 0.39 did not disable external entities when parsing XML from potentially untrusted sources. This may allow attackers to gain read access to otherwise protected resources, depending on how the library is used.	2021-07-09	5	CVE-2012-1102
xmlsoft -- libxml2	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.	2021-07-09	4	CVE-2021-3541
yop-poll -- yop_poll	In the YOP Poll WordPress plugin before 6.2.8, when a pool is created with the options "Allow other answers", "Display other answers in the result list" and "Show results", it can lead to Stored Cross-Site Scripting issues as the 'Other' answer is not sanitised before being output in the page. The execution of the XSS payload depends on the 'Show results' option selected, which could be before or after sending the vote for example.	2021-07-12	4.3	CVE-2021-24454 CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cms_made_simple	Cross Site Scripting (XSS) vulnerablity in CMS Made Simple 2.2.14 via the Logic field in the Content Manager feature.	2021-07-26	3.5	CVE-2020-23240 MISC
cmsmadesimple -- cms_made_simple	Cross Site Scripting (XSS) vulnerability in CMS Made Simple 2.2.14 in "Extra" via 'News > Article" feature.	2021-07-26	3.5	CVE-2020-23241 MISC
evo -- evolution_cms	Cross Site Scripting (XSS) vulnerability in Evolution CMS 2.0.2 via the Document Manager feature.	2021-07-26	3.5	CVE-2020-23238 MISC
lavalite -- lavalite	Cross Site Scripting (XSS) vulnerabiity exists in LavaLite CMS 5.8.0 via the Menu Blocks feature, which can be bypassed by using HTML event handlers, such as "ontoggle,".	2021-07-26	3.5	CVE-2020-23234 MISC
naviwebs -- navigatecms	Cross Site Scripting (XSS) vulnerability in NavigateCMS 2.9 when performing a Create or Edit via the Tools feature.	2021-07-26	3.5	CVE-2020-23242 MISC
naviwebs -- navigatecms	Cross Site Scripting (XSS) vulnerability in NavigateCMS NavigateCMS 2.9 via the name="wrong_path_redirect" feature.	2021-07-26	3.5	CVE-2020-23243 MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via /ipblacklist?errorip= (reflected).	2021-07-25	3.5	CVE-2021-37462 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via /extensionsinstruction?id= (reflected).	2021-07-25	3.5	CVE-2021-37461 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via /planprop?id= (reflected).	2021-07-25	3.5	CVE-2021-37460 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the customer name field (stored).	2021-07-25	3.5	CVE-2021-37459 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the primary phone field (stored).	2021-07-25	3.5	CVE-2021-37458 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the SipRule field (stored).	2021-07-25	3.5	CVE-2021-37457 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the blacklist IP address (stored).	2021-07-25	3.5	CVE-2021-37456 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the outbound dialing plan (stored).	2021-07-25	3.5	CVE-2021-37455 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the line name (stored).	2021-07-25	3.5	CVE-2021-37454 MISC MISC
nchsoftware -- axon_pbx	Cross Site Scripting (XSS) exists in NCH Axon PBX v2.22 and earlier via the extension name (stored).	2021-07-25	3.5	CVE-2021-37453 MISC MISC
nchsoftware -- ivm_attendant	Cross Site Scripting (XSS) exists in NCH IVM Attendant v5.12 and earlier via /msglist?mbx= (reflected).	2021-07-25	3.5	CVE-2021-37451 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nchsoftware -- ivm_attendant	Cross Site Scripting (XSS) exists in NCH IVM Attendant v5.12 and earlier via /ogmprop?id= (reflected).	2021-07-25	3.5	CVE-2021-37450 MISC MISC
nchsoftware -- quorum	In NCH Quorum v2.03 and earlier, XSS exists via User Display Name (stored).	2021-07-25	3.5	CVE-2021-37463 MISC MISC
nchsoftware -- quorum	In NCH Quorum v2.03 and earlier, XSS exists via Conference Description (stored).	2021-07-25	3.5	CVE-2021-37464 MISC MISC
nchsoftware -- quorum	In NCH Quorum v2.03 and earlier, XSS exists via /uploaddoc?id= (reflected).	2021-07-25	3.5	CVE-2021-37465 MISC MISC
nchsoftware -- quorum	In NCH Quorum v2.03 and earlier, XSS exists via /conference?id= (reflected).	2021-07-25	3.5	CVE-2021-37466 MISC MISC
nchsoftware -- quorum	In NCH Quorum v2.03 and earlier, XSS exists via /conferencebrowseuploadfile?confid= (reflected).	2021-07-25	3.5	CVE-2021-37467 MISC MISC
nchsoftware -- webdictate	In NCH WebDictate v2.13, persistent Cross Site Scripting (XSS) exists in the Recipient Name field. An authenticated user can add or modify the affected field to inject arbitrary JavaScript.	2021-07-25	3.5	CVE-2021-37470 MISC MISC
sourcecodester -- e-commerce_website	Cross-site scripting (XSS) vulnerability in SourceCodester E-Commerce Website v 1.0 allows remote attackers to inject arbitrary web script or HTM via the subject field to feedback_process.php.	2021-07-23	3.5	CVE-2021-25204 MISC
textpattern -- textpattern	Cross Site Scripting (XSS) vulnerability in Textpattern CMS 4.8.1 via Custom fields in the Menu Preferences feature.	2021-07-26	3.5	CVE-2020-23239 MISC