BULLETIN (SB21-060)
VULNERABILITY SUMMARY FOR THE WEEK OF
22ND FEBRUARY, 2021

Bulletin (SB21-060)
Vulnerability Summary for the Week of February 22, 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
alleghenycreative -- openrepeater	OpenRepeater (ORP) before 2.2 allows unauthenticated command injection via shell metacharacters in the functions/ajax_system.php post_service parameter.	2021-02-19	10	CVE-2019-25024 MISC MISC
amaze_file_manager_project -- amaze_file_manager	Amaze File Manager before 3.5.1 allows attackers to obtain root privileges via shell metacharacters in a symbolic link.	2021-02-19	7.2	CVE-2020-36246 MISC MISC
arubanetworks -- clearpass_policy_manager	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2021-02-23	9	CVE-2021-26679 MISC
arubanetworks -- clearpass_policy_manager	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2021-02-23	9	CVE-2021-26684 MISC
arubanetworks -- clearpass_policy_manager	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2021-02-23	9	CVE-2021-26683 MISC
arubanetworks -- clearpass_policy_manager	A remote authenticated command injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the ClearPass web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2021-02-23	9	CVE-2021-26680 MISC
arubanetworks -- clearpass_policy_manager	A local authenticated escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in ClearPass OnGuard could allow local authenticated users on a Windows platform to elevate their privileges. A successful exploit could allow an attacker to execute arbitrary code with SYSTEM level privileges.	2021-02-23	7.2	CVE-2021-26677 MISC
atlassian -- alfresco_enterprise_content_management	An issue was discovered in Alfresco Enterprise Content Management (ECM) before 6.2.1. A user with privileges to edit a FreeMarker template (e.g., a webscript) may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running Alfresco.	2021-02-19	9	CVE-2020-12873 MISC MISC
atlassian -- jira	An endpoint in Atlassian Jira Server for Slack plugin from version 0.0.3 before version 2.0.15 allows remote attackers to execute arbitrary code via a template injection vulnerability.	2021-02-22	9	CVE-2021-26068 MISC
bloodhound_project -- bloodhound	components/Modals/HelpTexts/GenericAll/GenericAll.jsx in Bloodhound <= 4.0.1 allows remote attackers to execute arbitrary system commands when the victim imports a malicious data file containing JavaScript in the objectId parameter.	2021-02-19	9.3	CVE-2021-3210 MISC MISC MISC

botan_project -- botan	In Botan before 2.17.3, constant-time computations are not used for certain decoding and encoding operations (base32, base58, base64, and hex).	2021-02-22	7.5	CVE-2021-24115 CONFIRM MISC MISC
collaboraoffice -- online	"loolforkit" is a privileged program that is supposed to be run by a special, non-privileged "lool" user. Before doing anything else "loolforkit" checks, if it was invoked by the "lool" user, and refuses to run with privileges, if it's not the case. In the vulnerable version of "loolforkit" this check was wrong, so a normal user could start "loolforkit" and eventually get local root privileges.	2021-02-23	7.2	CVE-2021-25630 MISC MISC
eyesofnetwork -- eyesofnetwork	EyesOfNetwork 5.3-10 uses an integer of between 8 and 10 digits for the session ID, which might be leveraged for brute-force authentication bypass (such as in CVE-2021-27513 exploitation).	2021-02-22	7.5	CVE-2021-27514 MISC MISC
geojson2kml_project -- geojson2kml	All versions of package geojson2kml are vulnerable to Command Injection via the index.js file. PoC: var a =require("geojson2kml"); a("./","& touch JHU",function(){})	2021-02-23	7.5	CVE-2020-28429 CONFIRM
inspur -- clusterengine	A Remote Code Execution vulnerability has been found in Inspur ClusterEngine V4.0. A remote attacker can send a malicious login packet to the control server	2021-02-22	10	CVE-2020-21224 MISC MISC
linux -- linux_kernel	A NULL pointer dereference flaw in Linux kernel versions prior to 5.11 may be seen if sco_sock_getsockopt function in net/bluetooth/sco.c do not have a sanity check for a socket connection, when using BT_SNDMTU/BT_RCVMTU for SCO sockets. This could allow a local attacker with a special user privilege to crash the system (DOS) or leak kernel internal information.	2021-02-19	7.2	CVE-2020-35499 MISC
microsoft -- .net	.NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26701.	2021-02-25	7.5	CVE-2021-24112 N/A
microsoft -- .net	.NET Core Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-24112.	2021-02-25	7.5	CVE-2021-26701 N/A
netshieldcorp -- nano_25_firmware	On Netshield NANO 25 10.2.18 devices, /usr/local/webmin/System/manual_ping.cgi allows OS command injection (after authentication by the attacker) because the system C library function is used unsafely.	2021-02-22	9	CVE-2021-3149 MISC MISC
nozominetworks -- central_management_control	OS Command Injection vulnerability when changing date settings or hostname using web GUI of Nozomi Networks Guardian and CMC allows authenticated administrators to perform remote code execution. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.	2021-02-22	9	CVE-2021-26724 CONFIRM
nuance-gulp-build-common_project -- nuance-gulp-build-common	All versions of package nuance-gulp-build-common are vulnerable to Command Injection via the index.js file. PoC: /var a = require("nuance-gulp-build-common") a.run("touch JHU")	2021-02-23	7.5	CVE-2020-28430 MISC
qualcomm -- apq8009	A buffer overflow can occur when playing an MKV clip due to lack of input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-02-22	7.5	CVE-2020-11283 CONFIRM
qualcomm -- apq8009_firmware	Out of bound memory access while playing music playbacks with crafted vorbis content due to improper checks in header extraction in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-02-22	10	CVE-2020-11170 CONFIRM

qualcomm -- apq8009_firmware	Out of bound write and read in TA while processing command from NS side due to improper length check on command and response buffers in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-02-22	7.2	CVE-2020-11195 CONFIRM
qualcomm -- apq8009_firmware	User can overwrite Security Code NV item without knowing current SPC due to improper validation of SPC code setting and device lock in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-02-22	7.2	CVE-2020-11177 CONFIRM
qualcomm -- apq8017_firmware	Possible buffer overflow while updating ikev2 parameters due to lack of check of input validation for certain parameters received from the ePDG server in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-02-22	10	CVE-2020-11163 CONFIRM
qualcomm -- aqt1000_firmware	Out of bound in camera driver due to lack of check of validation of array index before copying into array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-02-22	7.2	CVE-2020-11223 CONFIRM
qualcomm -- aqt1000_firmware	Possible out of bound access in TA while processing a command from NS side due to improper length check of response buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-02-22	7.2	CVE-2020-11194 CONFIRM
qualcomm -- aqt1000_firmware	Possible memory corruption in BSI module due to improper validation of parameter count in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile	2021-02-22	7.2	CVE-2020-11187 CONFIRM
redhat -- jboss_fuse	A flaw was found in the Undertow AJP connector. Malicious requests and abrupt connection closes could be triggered by an attacker using query strings with non-RFC compliant characters resulting in a denial of service. The highest threat from this vulnerability is to system availability. This affects Undertow 2.1.5.SP1, 2.0.33.SP2, and 2.2.3.SP1.	2021-02-23	7.8	CVE-2020-27782 MISC
redhat -- keycloak	A vulnerability was found in all versions of keycloak, where on using lower case HTTP headers (via cURL) we can bypass our Gatekeeper. Lower case headers are also accepted by some webservers (e.g. Jetty). This means there is no protection when we put a Gatekeeper in front of a Jetty server and use lowercase headers.	2021-02-23	7.5	CVE-2020-14359 MISC MISC
shinobi -- shinobi_pro	An issue was discovered in Shinobi through ocean version 1. lib/auth.js has Incorrect Access Control. Valid API Keys are held in an internal JS Object. Therefore an attacker can use JS Proto Method names (such as constructor or hasOwnProperty) to convince the System that the supplied API Key exists in the underlying JS object, and consequently achieve complete access to User/Admin/Super API functions, as demonstrated by a /super/constructor/accounts/list URI.	2021-02-22	7.5	CVE-2021-27228 MISC MISC MISC
smarty -- smarty	Smarty before 3.1.39 allows code injection via an unexpected function name after a {function name= substring.	2021-02-22	7.5	CVE-2021-26120 MISC
sytech -- xlreporter	An exploitable local privilege elevation vulnerability exists in the file system permissions of Sytech XL Reporter v14.0.1 install directory. Depending on the vector chosen, an attacker can overwrite service executables and execute arbitrary code with privileges of user set to run the service or replace other files within the installation folder, which would allow for local privilege escalation.	2021-02-19	7.2	CVE-2020-13549 MISC
theme-core_project -- theme-core	All versions of package theme-core are vulnerable to Command Injection via the lib/utils.js file, which is required by main entry of the package. PoC: var a =require("theme-core"); a.utils.sh("touch JHU")	2021-02-23	7.5	CVE-2020-28432 MISC
tribe29 -- checkmk	Checkmk before 1.6.0p17 allows local users to obtain SYSTEM privileges via a Trojan horse shell script in the %PROGRAMDATA%\checkmk\agent\local directory.	2021-02-19	7.2	CVE-2020-24908 MISC

wc-cmd_project -- wc-cmd	All versions of package wc-cmd are vulnerable to Command Injection via the index.js file. PoC: var a =require("wc-cmd"); a("touch JHU")	2021-02-23	7.5	CVE-2020-28431 MISC
yithemes -- woocommerce_gift_cards	An arbitrary file upload vulnerability in the YITH WooCommerce Gift Cards Premium plugin before 3.3.1 for WordPress allows remote attackers to achieve remote code execution on the operating system in the security context of the web server. In order to exploit this vulnerability, an attacker must be able to place a valid Gift Card product into the shopping cart. An uploaded file is placed at a predetermined path on the web server with a user-specified filename and extension. This occurs because the ywgc-upload-picture parameter can have a .php value even though the intention was to only allow uploads of Gift Card images.	2021-02-22	10	CVE-2021-3120 MISC MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acronis -- cyber_protect	An issue was discovered in Acronis Cyber Protect before 15 Update 1 build 26172. Because the local notification service misconfigures CORS, information disclosure can occur.	2021-02-22	5	CVE-2020-35556 MISC MISC
acronis -- cyber_protect	An issue was discovered in Acronis Cyber Protect before 15 Update 1 build 26172. There is cross-site scripting (XSS) in the console.	2021-02-22	4.3	CVE-2020-35664 MISC MISC
adobe -- acrobat	Acrobat Reader DC versions 2020.013.20066 (and earlier), 2020.001.30010 (and earlier) and 2017.011.30180 (and earlier) are affected by an information exposure vulnerability, that could enable an attacker to get a DNS interaction and track if the user has opened or closed a PDF file when loaded from the filesystem without a prompt. User interaction is required to exploit this vulnerability.	2021-02-23	4.3	CVE-2020-29075 CONFIRM
adobe -- bridge	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-02-25	6.8	CVE-2021-21065 MISC
adobe -- bridge	Adobe Bridge version 11.0 (and earlier) is affected by an out-of-bounds write vulnerability when parsing TTF files that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2021-02-25	6.8	CVE-2021-21066 MISC
advantech -- webaccess\/scada	The WADashboard component of WebAccess/SCADA Versions 9.0 and prior may allow an attacker to control or influence a path used in an operation on the filesystem and remotely execute code as an administrator.	2021-02-23	6.5	CVE-2020-25161 MISC
aida64 -- aida64	Buffer overflow in FinalWire Ltd AIDA64 Engineer 6.00.5100 allows attackers to execute arbitrary code by creating a crafted input that will overwrite the SEH handler.	2021-02-19	4.6	CVE-2020-19513 EXPLOIT-DB
apache -- myfaces	In the default configuration, Apache MyFaces Core versions 2.2.0 to 2.2.13, 2.3.0 to 2.3.7, 2.3-next-M1 to 2.3-next-M4, and 3.0.0-RC1 use cryptographically weak implicit and explicit cross-site request forgery (CSRF) tokens. Due to that limitation, it is possible (although difficult) for an attacker to calculate a future CSRF token value and to use that value to trick a user into executing unwanted actions on an application.	2021-02-19	6.8	CVE-2021-26296 MISC FULLDISC MISC
arubanetworks -- clearpass_policy_manager	A remote reflected cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the guest portal interface of ClearPass could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the portal. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the guest portal interface.	2021-02-23	4.3	CVE-2021-26682 MISC
arubanetworks -- clearpass_policy_manager	A remote authenticated SQL Injection vulnerabilitiy was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface API of ClearPass could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database.	2021-02-23	5.5	CVE-2021-26686 MISC
arubanetworks -- clearpass_policy_manager	A remote authenticated SQL Injection vulnerabilitiy was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in the web-based management interface API of ClearPass could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database.	2021-02-23	5.5	CVE-2021-26685 MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- clearpass_policy_manager	A local authenticated buffer overflow vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.8-HF1, 6.7.14-HF1. A vulnerability in ClearPass OnGuard could allow local authenticated users to cause a buffer overflow condition. A successful exploit could allow a local attacker to execute arbitrary code within the context the binary is running in, which is a lower privileged account.	2021-02-23	4.6	CVE-2020-7120 MISC
asus -- askey_rtf8115vw_firmware	Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow injection of a Host HTTP header.	2021-02-19	5.8	CVE-2021-27404 MISC
asus -- askey_rtf8115vw_firmware	Askey RTF8115VW BR_SV_g11.11_RTF_TEF001_V6.54_V014 devices allow cgi-bin/te_acceso_router.cgi curWebPage XSS.	2021-02-19	4.3	CVE-2021-27403 MISC
atlassian -- confluence	The ConfluenceResourceDownloadRewriteRule class in Confluence Server and Confluence Data Center before version 6.13.18, from 6.14.0 before 7.4.6, and from 7.5.0 before 7.8.3 allowed unauthenticated remote attackers to read arbitrary files within WEB-INF and META-INF directories via an incorrect path access check.	2021-02-22	5	CVE-2020-29448 MISC
carrier -- webctrl_system	Automated Logic Corporation (ALC) WebCTRL System 6.5 and prior allows remote attackers to execute any JavaScript code via a XSS payload for the first parameter in a GET request.	2021-02-22	4.3	CVE-2020-19762 MISC
chamilo -- chamilo	Chamilo 1.11.14 allows XSS via a main/calendar/agenda_list.php?type= URI.	2021-02-19	4.3	CVE-2021-26746 CONFIRM MISC MISC
cira -- canadian_shield	The CIRA Canadian Shield app before 4.0.13 for iOS lacks SSL Certificate Validation.	2021-02-23	4.3	CVE-2021-27189 MISC FULLDISC MISC
cnesty -- helpcom	Helpcom before v10.0 contains a file download and execution vulnerability caused by storing hardcoded cryptographic key. It finally leads to a file download and execution via access to crafted web page.	2021-02-24	6.8	CVE-2020-7846 CONFIRM
digium -- asterisk	A stack-based buffer overflow in res_rtp_asterisk.c in Sangoma Asterisk before 16.16.1, 17.x before 17.9.2, and 18.x before 18.2.1 and Certified Asterisk before 16.8-cert6 allows an authenticated WebRTC client to cause an Asterisk crash by sending multiple hold/unhold requests in quick succession. This is caused by a signedness comparison mismatch.	2021-02-19	4	CVE-2021-26713 MISC MISC MISC
djangoproject -- channels	Django Channels 3.x before 3.0.3 allows remote attackers to obtain sensitive information from a different request scope. The legacy channels.http.AsgiHandler class, used for handling HTTP type requests in an ASGI environment prior to Django 3.0, did not correctly separate request scopes in Channels 3.0. In many cases this would result in a crash but, with correct timing, responses could be sent to the wrong client, resulting in potential leakage of session identifiers and other sensitive data. Note that this affects only the legacy Channels provided class, and not Django's similar ASGIHandler, available from Django 3.0.	2021-02-22	5.8	CVE-2020-35681 CONFIRM MISC MISC
docsifyjs -- docsify	This affects the package docsify before 4.12.0. It is possible to bypass the remediation done by CVE-2020-7680 and execute malicious JavaScript through the following methods 1) When parsing HTML from remote URLs, the HTML code on the main page is sanitized, but this sanitization is not taking place in the sidebar. 2) The isURL external check can be bypassed by inserting more “////” characters	2021-02-19	4.3	CVE-2021-23342 MISC FULLDISC MISC MISC MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eyesofnetwork -- eyesofnetwork	The module admin_ITSM in EyesOfNetwork 5.3-10 allows remote authenticated users to upload arbitrary .xml.php files because it relies on "le filtre userside."	2021-02-22	6.5	CVE-2021-27513 MISC MISC
fujielectric -- v-server	The affected Fuji Electric V-Server Lite versions prior to 3.3.24.0 are vulnerable to an out-of-bounds write, which may allow an attacker to remotely execute arbitrary code.	2021-02-19	6.8	CVE-2020-25171 MISC
genymobile -- genymotion_desktop	** DISPUTED ** Genymotion Desktop through 3.2.0 leaks the host's clipboard data to the Android application by default. NOTE: the vendor's position is that this is intended behavior that can be changed through the Settings > Device screen.	2021-02-22	5	CVE-2021-27549 MISC MISC MISC MISC MISC MISC MISC
getgist -- chatbox	Chatbox is affected by cross-site scripting (XSS). An attacker has to upload any XSS payload with SVG, XML file in Chatbox. There is no restriction on file upload in Chatbox which leads to stored XSS.	2021-02-23	4.3	CVE-2020-35852 MISC MISC MISC
gnu -- glibc	The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.	2021-02-24	4.9	CVE-2021-27645 MISC
google -- chrome	Heap buffer overflow in Media in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21152 MISC MISC FEDORA
google -- chrome	Use after free in Payments in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21151 MISC MISC FEDORA
google -- chrome	Stack buffer overflow in Data Transfer in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21149 MISC MISC FEDORA
google -- chrome	Stack buffer overflow in GPU Process in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21153 MISC MISC FEDORA
google -- chrome	Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21150 MISC MISC FEDORA

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Heap buffer overflow in Tab Strip in Google Chrome prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21154 MISC MISC FEDORA
google -- chrome	Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21157 MISC MISC FEDORA
google -- chrome	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted script.	2021-02-22	6.8	CVE-2021-21156 MISC MISC FEDORA
google -- chrome	Heap buffer overflow in Tab Strip in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-02-22	6.8	CVE-2021-21155 MISC MISC FEDORA
google -- rendertron	Rendertron versions prior to 3.0.0 are are susceptible to a Server-Side Request Forgery (SSRF) attack. An attacker can use a specially crafted webpage to force a rendertron headless chrome process to render internal sites it has access to, and display it as a screenshot. Suggested mitigations are to upgrade your rendertron to version 3.0.0, or, if you cannot update, to secure the infrastructure to limit the headless chrome's access to your internal domain.	2021-02-23	4	CVE-2020-8902 CONFIRM
google -- slashify	The slashify package 1.0.0 for Node.js allows open-redirect attacks, as demonstrated by a localhost:3000///example.com/ substring.	2021-02-19	5.8	CVE-2021-3189 MISC MISC
hubspot -- jinjava	Jinjava before 2.5.4 allow access to arbitrary classes by calling Java methods on objects passed into a Jinjava context. This could allow for abuse of the application class loader, including Arbitrary File Disclosure.	2021-02-19	6.8	CVE-2020-12668 MISC MISC MISC MISC MISC
ibm -- planning_analytics	IBM Planning Analytics 2.0 could allow a remote authenticated attacker to obtain information about an organization's internal structure by exposing sensitive information in HTTP repsonses. IBM X-Force ID: 192029.	2021-02-23	4	CVE-2020-4953 XF CONFIRM
imagemagick -- imagemagick	In ImageMagick, there is an outside the range of representable values of type 'unsigned int' at MagickCore/quantum-private.h. This flaw affects ImageMagick versions prior to 7.0.9-0.	2021-02-23	4.3	CVE-2020-27768 MISC
intel -- bmc_firmware	Buffer overflow in the BMC firmware for some Intel(R) Server Boards, Server Systems and Compute Modules before version 2.47 may allow a privileged user to potentially enable escalation of privilege via local access.	2021-02-19	4.6	CVE-2020-12374 MISC
iptime -- nas-i_firmware	The ipTIME NAS product allows an arbitrary file upload vulnerability in the Manage Bulletins/Upload feature, which can be leveraged to gain remote code execution. This issue affects: pTIME NAS 1.4.36.	2021-02-23	5.2	CVE-2020-7847 CONFIRM

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jasper_project -- jasper	A flaw was found in jasper before 2.0.25. A null pointer dereference in jp2_decode in jp2_dec.c may lead to program crash and denial of service.	2021-02-23	4.3	CVE-2021-26927 MISC MISC
jasper_project -- jasper	A flaw was found in jasper before 2.0.25. An out of bounds read issue was found in jp2_decode function whic may lead to disclosure of information or program crash.	2021-02-23	5.8	CVE-2021-26926 MISC MISC
jenkins -- claim	A cross-site request forgery (CSRF) vulnerability in Jenkins Claim Plugin 2.18.1 and earlier allows attackers to change claims.	2021-02-24	4.3	CVE-2021-21620 CONFIRM
jenkins -- configuration_slicing	A cross-site request forgery (CSRF) vulnerability in Jenkins Configuration Slicing Plugin 1.51 and earlier allows attackers to apply different slice configurations.	2021-02-24	6.8	CVE-2021-21617 MLIST CONFIRM
jenkins -- support_core	Jenkins Support Core Plugin 2.72 and earlier provides the serialized user authentication as part of the "About user (basic authentication details only)" information, which can include the session ID of the user creating the support bundle in some configurations.	2021-02-24	5	CVE-2021-21621 CONFIRM
johnsoncontrols -- metasys_reporting_engine	Path Traversal vulnerability exists in Metasys Reporting Engine (MRE) Web Services which could allow a remote unauthenticated attacker to access and download arbitrary files from the system.	2021-02-19	5	CVE-2020-9050 CONFIRM CERT
kaco-newenergy -- xp100u_firmware	KACO New Energy XP100U Up to XP-JAVA 2.0 is affected by incorrect access control. Credentials will always be returned in plain-text from the local server during the KACO XP100U authentication process, regardless of whatever passwords have been provided, which leads to an information disclosure vulnerability.	2021-02-23	5	CVE-2021-3252 MISC MISC MISC
libxls_project -- libxls	An issue was discovered in libxls before and including 1.6.1 when reading Microsoft Excel files. A NULL pointer dereference vulnerability exists when parsing XLS cells in libxls/xls2csv.c:199. It could allow a remote attacker to cause a denial of service via crafted XLS file.	2021-02-23	4.3	CVE-2020-27819 MISC
linux -- linux_kernel	A use-after-free flaw was found in the io_uring in Linux kernel, where a local attacker with a user privilege could cause a denial of service problem on the system The issue results from the lack of validating the existence of an object prior to performing operations on the object by not incrementing the file reference counter while in use. The highest threat from this vulnerability is to data integrity, confidentiality and system availability.	2021-02-23	6.1	CVE-2021-20226 MISC
linux -- linux_kernel	There is a vulnerability in the linux kernel versions higher than 5.2 (if kernel compiled with config params CONFIG_BPF_SYSCALL=y , CONFIG_BPF=y , CONFIG_CGROUPS=y , CONFIG_CGROUP_BPF=y , CONFIG_HARDENED_USERCOPY not set, and BPF hook to getsockopt is registered). As result of BPF execution, the local user can trigger bug in __cgroup_bpf_run_filter_getsockopt() function that can lead to heap overflow (because of non-hardened usercopy). The impact of attack could be deny of service or possibly privileges escalation.	2021-02-23	4.6	CVE-2021-20194 MISC
luxion -- keyshot	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 have multiple NULL pointer dereference issues while processing project files, which may allow an attacker to execute arbitrary code.	2021-02-23	6.8	CVE-2021-22649 MISC
luxion -- keyshot	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions	2021-02-23	6.8	CVE-2021-22643 MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	prior to 10.1 are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.			
luxion -- keyshot	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to an attack because the .bip documents display a “load” command, which can be pointed to a .dll from a remote network share. As a result, the .dll entry point can be executed without sufficient UI warning.	2021-02-23	6.8	CVE-2021-22645 MISC
luxion -- keyshot	Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are vulnerable to multiple out-of-bounds write issues while processing project files, which may allow an attacker to execute arbitrary code.	2021-02-23	6.8	CVE-2021-22647 MISC
luxion -- keyshot	When loading a specially crafted file, Luxion KeyShot versions prior to 10.1, Luxion KeyShot Viewer versions prior to 10.1, Luxion KeyShot Network Rendering versions prior to 10.1, and Luxion KeyVR versions prior to 10.1 are, while processing the extraction of temporary files, suffering from a directory traversal vulnerability, which allows an attacker to store arbitrary scripts into automatic startup folders.	2021-02-23	6.8	CVE-2021-22651 MISC
mailtrain -- mailtrain	Mailtrain through 1.24.1 allows SQL Injection in statsClickedSubscribersByColumn in lib/models/campaigns.js via /campaigns/clicked/ajax because variable column names are not properly escaped.	2021-02-19	6	CVE-2020-24617 MISC MISC
mantisbt -- mantisbt	An issue was discovered in MantisBT through 2.24.3. In the helper_ensure_confirmed call in manage_custom_field_update.php, the custom field name is not sanitized. This may be problematic depending on CSP settings.	2021-02-22	4.3	CVE-2020-35571 MISC
mbsync_project -- mbsync	A flaw was found in mbsync before v1.3.5 and v1.4.1. Validations of the mailbox names returned by IMAP LIST/LSUB do not occur allowing a malicious or compromised server to use specially crafted mailbox names containing '..' path components to access data outside the designated mailbox on the opposite end of the synchronization channel. The highest threat from this vulnerability is to data confidentiality and integrity.	2021-02-23	5.8	CVE-2021-20247 MISC MISC
microsoft -- .net	.NET Core and Visual Studio Denial of Service Vulnerability	2021-02-25	4.3	CVE-2021-1721 N/A
microsoft -- modernflow	ModernFlow before 1.3.00.208 does not constrain web-page access to members of a security group, as demonstrated by the Search Screen and the Profile Screen.	2021-02-19	4	CVE-2021-3339 MISC MISC
nanohttpd -- nanohttpd	An issue was discovered in RouterNanoHTTPD.java in NanoHTTPD through 2.3.1. The GeneralHandler class implements a basic GET handler that prints debug information as an HTML page. Any web server that extends this class without implementing its own GET handler is vulnerable to reflected XSS, because the GeneralHandler GET handler prints user input passed through the query string without any sanitization.	2021-02-23	4.3	CVE-2020-13697 MISC MISC
nozominetworks -- central_management_control	Path Traversal vulnerability when changing timezone using web GUI of Nozomi Networks Guardian, CMC allows an authenticated administrator to read-protected system files. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.	2021-02-22	4	CVE-2021-26725 CONFIRM
openenergymonitor -- emoncms	Modules/input/Views/schedule.php in Emoncms through 10.2.7 allows XSS via the node parameter.	2021-02-21	4.3	CVE-2021-26716 MISC
osc -- open_ondemand	Open OnDemand before 1.5.7 and 1.6.x before 1.6.22 allows CSRF.	2021-02-19	6.8	CVE-2020-36247 MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
owncloud -- file_firewall	The File Firewall before 2.8.0 for ownCloud Server does not properly enforce file-type restrictions for public shares.	2021-02-19	5	CVE-2020-36249 MISC
owncloud -- owncloud	An issue was discovered in ownCloud before 10.4. Because of an SSRF issue (via the apps/files_sharing/external remote parameter), an authenticated attacker can interact with local services blindly (aka Blind SSRF) or conduct a Denial Of Service attack.	2021-02-19	6.5	CVE-2020-10252 MISC CONFIRM MISC
owncloud -- owncloud	An issue was discovered in ownCloud before 10.4. An attacker can bypass authentication on a password-protected image by displaying its preview.	2021-02-19	4.3	CVE-2020-10254 MISC CONFIRM MISC
owncloud -- owncloud	ownCloud Server before 10.3.0 allows an attacker, who has received non-administrative access to a group share, to remove everyone else's access to that share.	2021-02-19	4	CVE-2020-36251 MISC
png-img_project -- png-img	An integer overflow in the PngImg::InitStorage_() function of png-img before 3.1.0 leads to an under-allocation of heap memory and subsequently an exploitable heap-based buffer overflow when loading a crafted PNG file.	2021-02-20	6.8	CVE-2020-28248 MISC MISC MISC MISC
polarisoffice -- polaris_office	Polaris Office v9.102.66 is affected by a divide-by-zero error in PolarisOffice.exe and EngineDLL.dll that may cause a local denial of service. To exploit the vulnerability, someone must open a crafted PDF file.	2021-02-23	4.3	CVE-2021-27550 MISC
postgresql -- postgresql	A flaw was found in PostgreSQL in versions before 13.2, before 12.6, before 11.11, before 10.16, before 9.6.21 and before 9.5.25. This flaw allows a user with SELECT privilege on one column to craft a special query that returns all columns of the table. The highest threat from this vulnerability is to confidentiality.	2021-02-23	4	CVE-2021-20229 MISC
qualcomm -- apq8009	An Untrusted Pointer Dereference can occur while doing USB control transfers, if multiple requests of different standard request categories like device, interface & endpoint are made together. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-02-22	4.6	CVE-2020-11286 CONFIRM
qualcomm -- apq8009	Arithmetic overflow can happen while processing NOA IE due to improper error handling 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 Wired Infrastructure and Networking	2021-02-22	5	CVE-2020-11296 CONFIRM
qualcomm -- apq8009	Improper access control when using mmap with the kgsl driver with a special offset value that can be provided to map the memstore of the GPU to user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-02-22	4.6	CVE-2020-11282 CONFIRM
qualcomm -- aqt1000	Allowing RTT frames to be linked with non randomized MAC address by comparing the sequence numbers can lead to information disclosure. 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	2021-02-22	5	CVE-2020-11287 CONFIRM

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- aqt1000_firmware	Use after free issue in audio modules while removing and freeing objects during list iteration due to incorrect usage of macro in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile	2021-02-22	4.6	CVE-2020-11147 CONFIRM
redhat -- 3scale_api_management	A flaw was found in Red Hat 3scale API Management Platform 2. The 3scale backend does not perform preventive handling on user-requested date ranges in certain queries allowing a malicious authenticated user to submit a request with a sufficiently large date range to eventually yield an internal server error resulting in denial of service. The highest threat from this vulnerability is to system availability.	2021-02-23	6.8	CVE-2021-20252 MISC
redhat -- openshift_container_platform	A privilege escalation flaw was found in openshift4/ose-docker-builder. The build container runs with high privileges using a chrooted environment instead of runc. If an attacker can gain access to this build container, they can potentially utilize the raw devices of the underlying node, such as the network and storage devices, to at least escalate their privileges to that of the cluster admin. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-02-23	6.5	CVE-2021-20182 MISC
redhat -- openshift_installer	A flaw was found in the OpenShift Installer before version v0.9.0-master.0.20210125200451-95101da940b0. During installation of OpenShift Container Platform 4 clusters, bootstrap nodes are provisioned with anonymous authentication enabled on kubelet port 10250. A remote attacker able to reach this port during installation can make unauthenticated `/exec` requests to execute arbitrary commands within running containers. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-02-23	6.8	CVE-2021-20198 MISC
redhat -- satellite	A flaw was found in Red Hat Satellite. The BMC interface exposes the password through the API to an authenticated local attacker with view_hosts permission. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-02-23	4.6	CVE-2021-20256 MISC
scrapbox-parser_project -- scrapbox-parser	A ReDoS (regular expression denial of service) flaw was found in the @progfay/scrapbox-parser package before 6.0.3 for Node.js.	2021-02-19	5	CVE-2021-27405 MISC MISC MISC
se -- powerlogic_ion7400_firmware	A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION7700/73xx, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts Telnet network traffic between a user and the device.	2021-02-19	5	CVE-2021-22702 MISC
se -- powerlogic_ion7400_firmware	A CWE-319: Cleartext transmission of sensitive information vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause disclosure of user credentials when a malicious actor intercepts HTTP network traffic between a user and the device.	2021-02-19	5	CVE-2021-22703 MISC
smartstore -- smartstorenet	An issue was discovered in SmartStoreNET before 4.1.0. Lack of Cross Site Request Forgery (CSRF) protection may lead to elevation of privileges (e.g., /admin/customer/create to create an admin account).	2021-02-19	6.8	CVE-2020-27997 MISC MISC
smarty -- smarty	Smarty before 3.1.39 allows a Sandbox Escape because $smarty.template_object can be accessed in sandbox mode.	2021-02-22	5	CVE-2021-26119 MISC
snowsoftware -- snow_inventory	Snow Inventory Agent through 6.7.0 on Windows uses CPUID to report on processor types and versions that may be deployed and in use across an IT environment. A privilege-escalation vulnerability exists if CPUID is enabled, and thus it should be disabled via configuration settings.	2021-02-23	6.8	CVE-2021-27579 MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
softmaker -- planmaker_2021	A specially crafted document can cause the document parser to copy data from a particular record type into a static-sized buffer within an object that is smaller than the size used for the copy, which will cause a heap-based buffer overflow. An attacker can entice the victim to open a document to trigger this vulnerability. This affects SoftMaker Software GmbH SoftMaker Office PlanMaker 2021 (Revision 1014).	2021-02-23	6.8	CVE-2020-28587 MISC
stunnel -- stunnel	A flaw was found in stunnel before 5.57, where it improperly validates client certificates when it is configured to use both redirect and verifyChain options. This flaw allows an attacker with a certificate signed by a Certificate Authority, which is not the one accepted by the stunnel server, to access the tunneled service instead of being redirected to the address specified in the redirect option. The highest threat from this vulnerability is to confidentiality.	2021-02-23	5	CVE-2021-20230 MISC MISC
tasks -- tasks	"Tasks" application version before 9.7.3 is affected by insecure permissions. The VoiceCommandActivity application component allows arbitrary applications on a device to add tasks with no restrictions.	2021-02-22	4.6	CVE-2020-22475 MISC MISC
telegram -- telegram	The Terminate Session feature in the Telegram application through 7.2.1 for Android, and through 2.4.7 for Windows and UNIX, fails to invalidate a recently active session.	2021-02-19	5	CVE-2021-27351 MISC
twitter-stream_project -- twitter-stream	In voloko twitter-stream 0.1.10, missing TLS hostname validation allows an attacker to perform a man-in-the-middle attack against users of the library (because eventmachine is misused).	2021-02-19	4.3	CVE-2020-24392 MISC MISC
ui -- unifi_protect_controller	UniFi Protect before v1.17.1 allows an attacker to use spoofed cameras to perform a denial-of-service attack that may cause the UniFi Protect controller to crash.	2021-02-23	5	CVE-2021-22882 MISC MISC
urijs_project -- urijs	URI.js (aka urijs) before 1.19.6 mishandles certain uses of backslash such as http:\/ and interprets the URI as a relative path.	2021-02-22	5	CVE-2021-27516 MISC MISC
url-parse_project -- url-parse	url-parse before 1.5.0 mishandles certain uses of backslash such as http:\/ and interprets the URI as a relative path.	2021-02-22	5	CVE-2021-27515 MISC MISC MISC
we-con -- levistudiou	Multiple buffer overflow vulnerabilities exist when LeviStudioU (Version 2019-09-21 and prior) processes project files. Opening a specially crafted project file could allow an attacker to exploit and execute code under the privileges of the application.	2021-02-23	6.8	CVE-2020-16243 MISC
webware -- webdesktop	SSRF in the document conversion component of Webware Webdesktop 5.1.15 allows an attacker to read all files from the server.	2021-02-19	4	CVE-2021-3204 MISC
yeastar -- neogate_tg400_firmware	Yeastar NeoGate TG400 91.3.0.3 devices are affected by Directory Traversal. An authenticated user can decrypt firmware and can read sensitive information, such as a password or decryption key.	2021-02-19	4	CVE-2021-27328 MISC MISC MISC
yz1 -- yz1	Buffer overflow in Yz1 0.30 and 0.32, as used in IZArc 4.4, ZipGenius 6.3.2.3116, and Explzh (extension) 8.14, allows attackers to execute arbitrary code via a crafted archive file, related to filename handling.	2021-02-22	6.8	CVE-2020-24175 MISC MISC

MEDIUM Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
zohocorp -- manageengine_adselfservice_plus	A Server-side request forgery (SSRF) vulnerability in the ProductConfig servlet in Zoho ManageEngine ADSelfService Plus through 6013 allows a remote unauthenticated attacker to perform blind HTTP requests or perform a Cross-site scripting (XSS) attack against the administrative interface via an HTTP request, a different vulnerability than CVE-2019-3905.	2021-02-19	4.3	CVE-2021-27214 MISC MISC

LOW Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- livy	Livy server version 0.7.0-incubating (only) is vulnerable to a cross site scripting issue in the session name. A malicious user could use this flaw to access logs and results of other users' sessions and run jobs with their privileges. This issue is fixed in Livy 0.7.1-incubating.	2021-02-20	3.5	CVE-2021-26544 MLIST CONFIRM CONFIRM
appspace -- appspa	A stored XSS issue exists in Appspace 6.2.4. After a user is authenticated and enters an XSS payload under the groups section of the network tab, it is stored as the group name. Whenever another member visits that group, this payload executes.	2021-02-22	3.5	CVE-2021-27564 MISC
custom_global_vari ct -- custom_global	Stored cross-site scripting (XSS) in form field in robust.systems product Custom Global Variables v 1.0.5 allows a remote attacker to inject arbitrary code via the vars[0][name] field.	2021-02-25	3.5	CVE-2021-3124 MISC MISC
dell -- emc_powerprotect very	Dell EMC PowerProtect Cyber Recovery, version 19.7.0.1, contains an Information Disclosure vulnerability. A locally authenticated high privileged Cyber Recovery user may potentially exploit this vulnerability leading to the takeover of the notification email account.	2021-02-19	3.6	CVE-2021-21512 MISC
fastadmin -- fastadr	fastadmin V1.0.0.20200506_beta contains a cross-site scripting (XSS) vulnerability which may allow an attacker to obtain administrator credentials to log in to the background.	2021-02-23	3.5	CVE-2020-26609 MISC MISC MISC
jenkins -- active_ch	Jenkins Active Choices Plugin 2.5.2 and earlier does not escape reference parameter values, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	2021-02-24	3.5	CVE-2021-21616 MLIST CONFIRM
jenkins -- artifact_repository_	Jenkins Artifact Repository Parameter Plugin 1.0.0 and earlier does not escape parameter names and descriptions, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	2021-02-24	3.5	CVE-2021-21622 CONFIRM
jenkins -- claim	Jenkins Claim Plugin 2.18.1 and earlier does not escape the user display name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers who are able to control the display names of Jenkins users, either via the security realm, or directly inside Jenkins.	2021-02-24	3.5	CVE-2021-21619 MLIST CONFIRM
jenkins -- repository	Jenkins Repository Connector Plugin 2.0.2 and earlier does not escape parameter names and descriptions for past builds, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2021-02-24	3.5	CVE-2021-21618 CONFIRM
keybase -- keybase	Keybase Desktop Client before 5.6.0 on Windows and macOS, and before 5.6.1 on Linux, allows an attacker to obtain potentially sensitive media (such as private pictures) in the Cache and uploadtemps directories. It fails to effectively clear cached pictures, even after deletion via normal methodology within the client, or by utilizing the "Explode message/Explode now" functionality. Local filesystem access is needed by the attacker.	2021-02-23	2.1	CVE-2021-23827 MISC MISC MISC
lightcms_project --	A stored-self XSS exists in LightCMS v1.3.4, allowing an attacker to execute HTML or JavaScript code in a vulnerable Title field to /admin/SensitiveWords.	2021-02-24	3.5	CVE-2021-3355 MISC MISC
monicahq -- monica	The Contact page in Monica 2.19.1 allows stored XSS via the First Name field.	2021-02-22	3.5	CVE-2021-27368 MISC MISC
monicahq -- monica	The Contact page in Monica 2.19.1 allows stored XSS via the Last Name field.	2021-02-22	3.5	CVE-2021-27370 MISC

				MISC MISC
monicahq -- monica	The Contact page in Monica 2.19.1 allows stored XSS via the Description field.	2021-02-22	3.5	CVE-2021-27371 MISC MISC
monicahq -- monica	The Contact page in Monica 2.19.1 allows stored XSS via the Nickname field.	2021-02-22	3.5	CVE-2021-27559 MISC MISC
monicahq -- monica	The Contact page in Monica 2.19.1 allows stored XSS via the Middle Name field.	2021-02-22	3.5	CVE-2021-27369 MISC MISC
mybb -- mybb	MyBB before 1.8.25 allows stored XSS via nested [email] tags with MyCode (aka BBCode).	2021-02-22	3.5	CVE-2021-27279 CONFIRM CONFIRM MISC
owncloud -- ownclo	ownCloud Server 10.x before 10.3.1 allows an attacker, who has one outgoing share from a victim, to access any version of any file by sending a request for a predictable ID number.	2021-02-19	2.7	CVE-2020-36252 MISC
owncloud -- ownclo	The ownCloud application before 2.15 for Android allows attackers to use adb to include a PIN preferences value in a backup archive, and consequently bypass the PIN lock feature by restoring from this archive.	2021-02-19	2.1	CVE-2020-36248 MISC
owncloud -- ownclo	In the ownCloud application before 2.15 for Android, the lock protection mechanism can be bypassed by moving the system date/time into the past.	2021-02-19	2.1	CVE-2020-36250 MISC
se -- powerlogic_ion740	A CWE-352: Cross-Site Request Forgery vulnerability exists in PowerLogic ION7400, ION7650, ION83xx/84xx/85xx/8600, ION8650, ION8800, ION9000 and PM800 (see notification for affected versions), that could cause a user to perform an unintended action on the target device when using the HTTP web interface.	2021-02-19	3.5	CVE-2021-22701 MISC