BULLETIN (SB20-244)
VULNERABILITY SUMMARY FOR THE WEEK OF 31ST AUGUST, 2020

Bulletin (SB20-244)
Vulnerability Summary for the Week of August 31, 2020

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
13enforme -- 13enforme_cms	13enforme CMS 1.0 has SQL Injection via the 'content.php' id parameter.	2020-08-27	7.5	CVE-2020-23979 MISC
cellopoint -- cellos	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly. With the cookie of the system administrator, attackers can inject and remotely execute arbitrary command to manipulate the system.	2020-08-25	9	CVE-2020-17384 MISC
ibm -- connect\	IBM Sterling Connect:Direct for UNIX 4.2.0, 4.3.0, 6.0.0, and 6.1.0 is vulnerable to a stack based buffer ovreflow, caused by improper bounds checking. A local attacker could manipulate CD UNIX to obtain root provileges. IBM X-Force ID: 184578.	2020-08-24	7.2	CVE-2020-4587 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 172084.	2020-08-26	9	CVE-2019-4713 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171832.	2020-08-26	7.5	CVE-2019-4694 XF CONFIRM
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the isHPSmartComponent method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10501.	2020-08-25	9	CVE-2020-15642 MISC MISC
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the saveAsText method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10549.	2020-08-25	9	CVE-2020-15643 MISC MISC

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the setAppFileBytes method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10550.	2020-08-25	9	CVE-2020-15644 MISC MISC
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getFileFromURL method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10553.	2020-08-25	9	CVE-2020-15645 MISC MISC
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the writeObjectToConfigFile method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10565.	2020-08-25	9	CVE-2020-17387 MISC MISC
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Tomcat configuration file. The issue results from the lack of proper restriction to the Tomcat admin console. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10799.	2020-08-25	9	CVE-2020-17388 MISC MISC
marvell -- qconvergeconsole	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the decryptFile method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10502.	2020-08-25	9	CVE-2020-17389 MISC MISC
moog -- exvf5c-2_firmware	The Moog EXO Series EXVF5C-2 and EXVP7C2-3 units support the ONVIF interoperability IP-based physical security protocol, which requires authentication for some of its operations. It was found that the authentication check for those ONVIF operations can be	2020-08-21	10	CVE-2020-24051

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bypassed. An attacker can abuse this issue to execute privileged operations without authentication, for instance, to create a new Administrator user.			MISC MISC
moog -- exvf5c-2_firmware	The administration console of the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units features a 'statusbroadcast' command that can spawn a given process repeatedly at a certain time interval as 'root'. One of the limitations of this feature is that it only takes a path to a binary without arguments; however, this can be circumvented using special shell variables, such as '${IFS}'. As a result, an attacker can execute arbitrary commands as 'root' on the units.	2020-08-21	10	CVE-2020-24054 MISC MISC
ncr -- aptra_xfs	NCR SelfServ ATMs running APTRA XFS 05.01.00 or earlier do not authenticate or protect the integrity of USB HID communications between the currency dispenser and the host computer, permitting an attacker with physical access to internal ATM components the ability to inject a malicious payload and execute arbitrary code with SYSTEM privileges on the host computer by causing a buffer overflow on the host.	2020-08-21	7.2	CVE-2020-9063 MISC MISC MISC MISC MISC
ncr -- aptra_xfs	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not properly validate softare updates for the bunch note acceptor (BNA), enabling an attacker with physical access to internal ATM components to restart the host computer and execute arbitrary code with SYSTEM privileges because while booting, the update process looks for CAB archives on removable media and executes a specific file without first validating the signature of the CAB archive.	2020-08-21	7.2	CVE-2020-10126 MISC MISC
nextcloud -- nextcloud	Missing sanitization of a server response in Nextcloud Desktop Client 2.6.4 for Linux allowed a malicious Nextcloud Server to store files outside of the dedicated sync directory.	2020-08-21	7.1	CVE-2020-8227 MISC MISC
safe-eval_project -- safe-eval	This affects all versions of package safe-eval. It is possible for an attacker to run an arbitrary command on the host machine.	2020-08-21	7.5	CVE-2020-7710 MISC MISC
sierrawireless -- aleos	A buffer overflow exists in the SMS handler API of ALEOS before 4.13.0, 4.9.5, 4.9.4 that may allow code execution as root.	2020-08-21	9	CVE-2019-11859 MISC
sintef -- urx	Universal Robots controller execute URCaps (zip files containing Java-powered applications) without any permission restrictions and a wide API that presents many primitives that can compromise	2020-08-21	7.2	CVE-2020-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the overall robot operations as demonstrated in our video. In our PoC we demonstrate how a malicious actor could 'cook' a custom URCap that when deployed by the user (intendedly or unintendedly) compromises the system			10290 CONFIRM
softing -- opc	Softing Industrial Automation all versions prior to the latest build of version 4.47.0, The affected product is vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.	2020-08-25	7.5	CVE-2020-14524 MISC
soluzioneglobale -- ecommerce_cms	SQL injection can occur in Soluzione Globale Ecommerce CMS v1 via the parameter " offerta.php"	2020-08-27	7.5	CVE-2020-23978 MISC MISC
verint -- 5620ptz_firmware	Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666. The service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication.	2020-08-21	7.5	CVE-2020-24055 MISC MISC
verint -- s5120fd_firmware	The management website of the Verint S5120FD Verint_FW_0_42 unit features a CGI endpoint ('ipfilter.cgi') that allows the user to manage network filtering on the unit. This endpoint is vulnerable to a command injection. An authenticated attacker can leverage this issue to execute arbitrary commands as 'root'.	2020-08-21	9	CVE-2020-24057 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
13enforme -- 13enforme_cms	13enforme CMS 1.0 has Cross Site Scripting via the "content.php" id parameter.	2020-08-27	4.3	CVE-2020-23981 MISC
asus -- rt-ac1900p_firmware	An issue was discovered on ASUS RT-AC1900P routers before 3.0.0.4.385_20253. They allow XSS via spoofed Release Notes on the Firmware Upgrade page.	2020-08-26	4.3	CVE-2020-15499 MISC
cellopoint -- cellos	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly. With cookie of an authenticated user, attackers can temper with the URL parameter and access arbitrary file on system.	2020-08-25	4	CVE-2020-17386 MISC
cellopoint -- cellos	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly, which allows unauthorized user to launch Path Traversal attack and access arbitrate file on the system.	2020-08-25	5	CVE-2020-17385 MISC
cisco -- data_center_network_manager	A vulnerability in a specific REST API method of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a path traversal attack on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	2020-08-26	5.5	CVE-2020-3519 CISCO
cisco -- data_center_network_manager	A vulnerability in a specific REST API of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker with a low-privileged account could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to read arbitrary files on the affected system.	2020-08-26	4	CVE-2020-3521 CISCO
cloudfoundry -- cf-deployment	Cloud Foundry Routing (Gorouter), versions prior to 0.204.0, when used in a deployment with NGINX reverse proxies in front of the Gorouters, is potentially vulnerable to denial-of-service attacks in which an unauthenticated malicious attacker can send specially-crafted HTTP requests that may cause the Gorouters to be dropped from the NGINX backend pool.	2020-08-21	4	CVE-2020-5416 CONFIRM
cloudfoundry -- cf-deployment	Cloud Foundry CAPI (Cloud Controller), versions prior to 1.97.0, when used in a deployment where an app domain is also the system domain (which is true in the default CF Deployment manifest), were vulnerable to developers maliciously or accidentally claiming certain sensitive routes, potentially resulting in the developer's app handling some requests that were expected to go to certain system components.	2020-08-21	6.5	CVE-2020-5417 CONFIRM
codiad -- codiad	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** A Cross Site Scripting (XSS) vulnerability was found in Codiad v1.7.8 and later. The vulnerability occurs because of improper sanitization of the folder's name $path variable in components/filemanager/class.filemanager.php. NOTE: the vendor states "Codiad is no longer under active maintenance by core contributors."	2020-08-25	4.3	CVE-2020-14042 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cogboard -- red_discord_bot	In Red Discord Bot before version 3.3.11, a RCE exploit has been discovered in the Trivia module: this exploit allows Discord users with specifically crafted usernames to inject code into the Trivia module's leaderboard command. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. This critical exploit has been fixed on version 3.3.11.	2020-08-21	5.5	CVE-2020-15140 MISC CONFIRM
cogboard -- red_discord_bot	Red Discord Bot before versions 3.3.12 and 3.4 has a Remote Code Execution vulnerability in the Streams module. This exploit allows Discord users with specifically crafted "going live" messages to inject code into the Streams module's going live message. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. As a workaround, unloading the Trivia module with `unload streams` can render this exploit not accessible. It is highly recommended updating to 3.3.12 or 3.4 to completely patch this issue.	2020-08-21	6	CVE-2020-15147 MISC MISC CONFIRM
cybersolutions -- cybermail	Cross-site scripting vulnerability in CyberMail Ver.6.x and Ver.7.x allows remote attackers to inject arbitrary script or HTML via a specially crafted URL.	2020-08-25	4.3	CVE-2020-5540 MISC MISC
cybersolutions -- cybermail	Open redirect vulnerability in CyberMail Ver.6.x and Ver.7.x allows remote attackers to redirect users to arbitrary sites and conduct phishing attacks via a specially crafted URL.	2020-08-25	5.8	CVE-2020-5541 MISC MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function form 'Name' in dbhcms\types.php, A remote unauthenticated attacker can exploit this vulnerability to hijack other users.	2020-08-24	4.3	CVE-2020-19880 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php line 107,	2020-08-24	4.3	CVE-2020-19879 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a sensitive information leaks vulnerability as there is no security access control in /dbhcms/ext/news/ext.news.be.php, A remote unauthenticated attacker can exploit this vulnerability to get path information.	2020-08-24	5	CVE-2020-19878 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a directory traversal vulnerability as there is no directory control function in directory /dbhcms/. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2020-08-24	5	CVE-2020-19877 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has an unauthorized operation vulnerability because there's no access control at line 175 of dbhcms\page.php for empty cache operation. This vulnerability can be exploited to empty a table.	2020-08-24	4.3	CVE-2020-19888 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has an Arbitrary file read vulnerability in dbhcms\mod\mod.editor.php $_GET['file'] is filename,and as there is no filter function for security, you can read any file's content.	2020-08-24	4	CVE-2020-19890 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dbhcms_project -- dbhcms	DBHcms v1.2.0 has an Arbitrary file write vulnerability in dbhcms\mod\mod.editor.php $_POST['updatefile'] is filename and $_POST['tinymce_content'] is file content, there is no filter function for security. A remote authenticated admin user can exploit this vulnerability to get a webshell.	2020-08-24	6.5	CVE-2020-19891 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for index.php?dbhcms_pid=-70 can add a user.	2020-08-24	6.8	CVE-2020-19889 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for an /index.php?dbhcms_pid=-80&deletemenu=9 can delete any menu.	2020-08-24	4.3	CVE-2020-19886 MISC
dolibarr -- dolibarr	Dolibarr CRM before 11.0.5 allows privilege escalation. This could allow remote authenticated attackers to upload arbitrary files via societe/document.php in which "disabled" is changed to "enabled" in the HTML source code.	2020-08-21	4	CVE-2020-14201 CONFIRM MISC
elementor -- elementor_page_builder	Elementor 2.9.5 and below WordPress plugin allows authenticated users to activate its safe mode feature. This can be exploited to disable all security plugins on the blog.	2020-08-21	4	CVE-2020-20634 MISC
gog -- galaxy	The client (aka GalaxyClientService.exe) in GOG GALAXY through 2.0.20 allows local privilege escalation from any authenticated user to SYSTEM by instructing the Windows service to execute arbitrary commands. This occurs because the attacker can inject a DLL into GalaxyClient.exe, defeating the TCP-based "trusted client" protection mechanism.	2020-08-21	6.9	CVE-2020-24574 MISC MISC MISC
goxmldsig_project -- goxmldsig	This affects all versions of package github.com/russellhaering/goxmldsig. There is a crash on nil-pointer dereference caused by sending malformed XML signatures.	2020-08-23	5	CVE-2020-7711 MISC MISC
huawei -- fusioncompute	FusionCompute 8.0.0 has an information leak vulnerability. A module does not launch strict access control and information protection. Attackers with low privilege can get some extra information. This can lead to information leak.	2020-08-21	4	CVE-2020-9246 MISC
ibm -- elastic_storage_server	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment while configuring some of the network services. IBM X-Force ID: 179165.	2020-08-24	4	CVE-2020-4383 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 171822.	2020-08-26	5	CVE-2019-4686 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 stores user credentials in plain in clear text which can be read by an authenticated user. IBM X-Force ID: 171938.	2020-08-26	4	CVE-2019-4697

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 171825.	2020-08-26	4.3	CVE-2019-4688 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 generates an error message that includes sensitive information about its environment, users, or associated data. IBM X-Force ID: 171931.	2020-08-26	4	CVE-2019-4699 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 171826.	2020-08-26	5	CVE-2019-4689 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 171829.	2020-08-26	5	CVE-2019-4692 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 171929.	2020-08-26	5	CVE-2019-4698 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 171936.	2020-08-26	5	CVE-2019-4701 XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 10.5, 10.6, and 11.0 could allow an unauthorized user to obtain sensitive information due to missing security controls. IBM X-Force ID: 141226.	2020-08-26	5	CVE-2018-1501 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 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. IBM X-Force ID: 174402.	2020-08-27	5	CVE-2020-4166 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 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: 174406.	2020-08-24	4.3	CVE-2020-4170 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 174407.	2020-08-27	4	CVE-2020-4171 XF CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174683.	2020-08-27	5	CVE-2020-4174 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174405.	2020-08-27	5	CVE-2020-4169 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 174408.	2020-08-27	5	CVE-2020-4172 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 184880.	2020-08-27	6.5	CVE-2020-4603 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 could allow an attacker to obtain sensitive information or perform unauthorized actions due to improper authenciation mechanisms. IBM X-Force ID: 174403.	2020-08-27	6.4	CVE-2020-4167 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 184823.	2020-08-24	5.8	CVE-2020-4598 XF CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server ND 8.5 and 9.0, and IBM WebSphere Virtual Enterprise 7.0 and 8.0 are vulnerable to cross-site scripting when High Availability Deployment Manager is configured.	2020-08-27	4.3	CVE-2020-4575 XF CONFIRM
instructure -- canvas_learning_management_service	Server-Side Request Forgery in Canvas LMS 2020-07-29 allows a remote, unauthenticated attacker to cause the Canvas application to perform HTTP GET requests to arbitrary domains.	2020-08-21	5	CVE-2020-5775 MISC
isc -- bind	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker	2020-08-21	4.3	CVE-2020-8623 CONFIRM MLIST FEDORA FEDORA GENTOO CONFIRM UBUNTU DEBIAN CONFIRM
isc -- bind	In BIND 9.14.0 -> 9.16.5, 9.17.0 -> 9.17.3, If a server is configured with both QNAME minimization and 'forward first' then an attacker who	2020-08-21	4.3	CVE-2020-8621

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can send queries to it may be able to trigger the condition that will cause the server to crash. Servers that 'forward only' are not affected.			CONFIRM GENTOO CONFIRM UBUNTU CONFIRM
isc -- bind	In BIND 9.15.6 -> 9.16.5, 9.17.0 -> 9.17.3, An attacker who can establish a TCP connection with the server and send data on that connection can exploit this to trigger the assertion failure, causing the server to exit.	2020-08-21	5	CVE-2020-8620 CONFIRM GENTOO CONFIRM UBUNTU CONFIRM
isc -- bind	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of the packet and message, and spoof a truncated response to trigger an assertion failure, causing the server to exit.	2020-08-21	4	CVE-2020-8622 CONFIRM MLIST FEDORA FEDORA GENTOO CONFIRM UBUNTU UBUNTU DEBIAN CONFIRM
isc -- bind	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone.	2020-08-21	4	CVE-2020-8624 CONFIRM FEDORA FEDORA GENTOO CONFIRM UBUNTU DEBIAN CONFIRM
joomla -- joomla\!	An issue was discovered in Joomla! before 3.9.21. Lack of input validation in the vote feature of com_content leads to an open redirect.	2020-08-26	5.8	CVE-2020-24598 MISC
joomla -- joomla\!	An issue was discovered in Joomla! before 3.9.21. Lack of escaping in mod_latestactions allows XSS attacks.	2020-08-26	4.3	CVE-2020-24599 MISC
marvell -- qconvergeconsole	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getFileUploadBytes method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10499.	2020-08-25	5	CVE-2020-15641 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
marvell -- qconvergeconsole	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getFileUploadBytes method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10497.	2020-08-25	5	CVE-2020-15640 MISC MISC
mongodb -- mongodb	A user authorized to perform database queries may cause denial of service by issuing specially crafted queries, which violate an invariant in the query subsystem's support for geoNear. This issue affects: MongoDB Inc. MongoDB Server v4.5 versions prior to 4.5.1; v4.4 versions prior to 4.4.0-rc7; v4.2 versions prior to 4.2.8; v4.0 versions prior to 4.0.19.	2020-08-21	4	CVE-2020-7923 MISC MLIST
moog -- exvf5c-2_firmware	Moog EXO Series EXVF5C-2 and EXVP7C2-3 units have a hardcoded credentials vulnerability. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols.	2020-08-21	5	CVE-2020-24053 MISC MISC
moog -- exvf5c-2_firmware	Several XML External Entity (XXE) vulnerabilities in the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units allow remote unauthenticated users to read arbitrary files via a crafted Document Type Definition (DTD) in an XML request.	2020-08-21	6.4	CVE-2020-24052 MISC MISC
ncr -- aptra_xfs	NCR SelfServ ATMs running APTRA XFS 04.02.01 and 05.01.00 implement 512-bit RSA certificates to validate bunch note acceptor (BNA) software updates, which can be broken by an attacker with physical access in a sufficiently short period of time, thereby enabling the attacker to sign arbitrary files and CAB archives used to update BNA software, as well as bypass application whitelisting, resulting in the ability to execute arbitrary code.	2020-08-21	4.6	CVE-2020-10125 MISC MISC
ncr -- aptra_xfs	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not encrypt, authenticate, or verify the integrity of messages between the BNA and the host computer, which could allow an attacker with physical access to the internal components of the ATM to execute arbitrary code, including code that enables the attacker to commit deposit forgery.	2020-08-21	4.4	CVE-2020-10124 MISC MISC
nexusdb -- nexusdb	NexusQA NexusDB before 4.50.23 allows the reading of files via ../ directory traversal.	2020-08-21	5	CVE-2020-24571 MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11304.	2020-08-25	4.6	CVE-2020-17400 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the prl_naptd process. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11134.	2020-08-25	4.6	CVE-2020-17395 MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.3-47255. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handler for HOST_IOCTL_SET_KERNEL_SYMBOLS in the prl_hypervisor kext. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-10519.	2020-08-25	4.6	CVE-2020-17392 MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor module. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-11217.	2020-08-25	4.6	CVE-2020-17396 MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-11303.	2020-08-25	4.6	CVE-2020-17399 MISC MISC
philips -- dreammapper	Philips DreamMapper, Version 2.24 and prior. Information written to log files can give guidance to a potential attacker.	2020-08-21	5	CVE-2020-14518 MISC
philips -- suresigns_vs4_firmware	Philips SureSigns VS4, A.07.107 and prior. When an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct.	2020-08-21	4	CVE-2020-16239 MISC
postgresql -- postgresql	It was found that PostgreSQL versions before 12.4, before 11.9 and before 10.14 did not properly sanitize the search_path during logical replication. An authenticated attacker could use this flaw in an attack similar to CVE-2018-1058, in order to execute arbitrary SQL command in the context of the user used for replication.	2020-08-24	6.5	CVE-2020-14349 SUSE SUSE SUSE MISC GENTOO

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
postgresql -- postgresql	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23.	2020-08-24	4.4	CVE-2020-14350 SUSE SUSE SUSE SUSE MISC DEBIAN GENTOO
redhat -- ansible	A flaw was found in the solaris_zone module from the Ansible Community modules. When setting the name for the zone on the Solaris host, the zone name is checked by listing the process with the 'ps' bare command on the remote machine. An attacker could take advantage of this flaw by crafting the name of the zone and executing arbitrary commands in the remote host. Ansible Engine 2.7.15, 2.8.7, and 2.9.2 as well as previous versions are affected.	2020-08-26	6.1	CVE-2019-14904 MISC MISC
secomea -- gatemanager_8250_firmware	GateManager versions prior to 9.2c, The affected product uses a weak hash type, which may allow an attacker to view user passwords.	2020-08-25	5	CVE-2020-14512 MISC
sierrawireless -- aleos	Multiple buffer overflow vulnerabilities exist in the AceManager Web API of ALEOS before 4.13.0, 4.9.5, and 4.4.9.	2020-08-21	6.5	CVE-2019-11858 MISC
sierrawireless -- aleos	The SSH service on ALEOS before 4.12.0, 4.9.5, 4.4.9 allows traffic proxying.	2020-08-21	4.6	CVE-2019-11862 MISC
sierrawireless -- aleos	Lack of input sanitization in AceManager of ALEOS before 4.12.0, 4.9.5 and 4.4.9 allows disclosure of sensitive system information.	2020-08-21	4	CVE-2019-11857 MISC
softing -- opc	Softing Industrial Automation all versions prior to the latest build of version 4.47.0, The affected product is vulnerable to uncontrolled resource consumption, which may allow an attacker to cause a denial-of-service condition.	2020-08-25	5	CVE-2020-14522 MISC
techkshetrainfo -- savsoft_quiz	TechKshetra Info Solutions Pvt. Ltd Savsoft Quiz 5 has XSS which can result in an attacker injecting the XSS payload in the User Registration section and each time the admin visits the manage user section from the admin panel, the XSS triggers and the attacker can steal the cookie via crafted payload.	2020-08-25	4.3	CVE-2020-24609 MISC
verint -- 5620ptz_firmware	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols.	2020-08-21	5	CVE-2020-24056 MISC MISC
vmware -- cloud_foundation	VMware ESXi and vCenter Server contain a partial denial of service vulnerability in their respective authentication services. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.3.	2020-08-21	5	CVE-2020-3976 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webdesi9 -- file_manager	mndpsingh287 WP File Manager v6.4 and lower fails to restrict external access to the fm_backups directory with a .htaccess file. This results in the ability for unauthenticated users to browse and download any site backups, which sometimes include full database backups, that the plugin has taken.	2020-08-26	5	CVE-2020-24312 MISC
wolfssl -- wolfssl	An issue was discovered in wolfSSL before 4.5.0. It mishandles the change_cipher_spec (CCS) message processing logic for TLS 1.3. If an attacker sends ChangeCipherSpec messages in a crafted way involving more than one in a row, the server becomes stuck in the ProcessReply() loop, i.e., a denial of service.	2020-08-21	5	CVE-2020-12457 MISC CONFIRM
wolfssl -- wolfssl	An issue was discovered in wolfSSL before 4.5.0, when single precision is not employed. Local attackers can conduct a cache-timing attack against public key operations. These attackers may already have obtained sensitive information if the affected system has been used for private key operations (e.g., signing with a private key).	2020-08-21	6.9	CVE-2020-15309 CONFIRM
wolfssl -- wolfssl	An issue was discovered in the DTLS handshake implementation in wolfSSL before 4.5.0. Clear DTLS application_data messages in epoch 0 do not produce an out-of-order error. Instead, these messages are returned to the application.	2020-08-21	5	CVE-2020-24585 MISC MISC
wso2 -- api_manager	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML External Entity injection (XXE) attacks.	2020-08-21	6.4	CVE-2020-24589 MISC
wso2 -- api_manager	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML Entity Expansion attacks.	2020-08-21	6.4	CVE-2020-24590 MISC
wso2 -- api_manager	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through 3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0, Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0.	2020-08-21	5.5	CVE-2020-24591 MISC
zulip -- zulip_server	Zulip Server 2.x before 2.1.7 allows eval injection if a privileged attacker were able to write directly to the postgres database, and chose to write a crafted custom profile field value.	2020-08-21	6.5	CVE-2020-15070 CONFIRM
zulip -- zulip_server	Zulip Server before 2.1.5 allows reverse tabnapping via a topic header link.	2020-08-21	5.8	CVE-2020-14194 CONFIRM
zulip -- zulip_server	Zulip Server before 2.1.5 has Incorrect Access Control because 0198_preregistrationuser_invited_as adds the administrator role to invitations.	2020-08-21	5	CVE-2020-14215 CONFIRM
zulip -- zulip_server	Zulip Server before 2.1.5 allows reflected XSS via the Dropbox webhook.	2020-08-21	4.3	CVE-2020-12759 CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- data_center_network_manager	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2020-08-26	3.5	CVE-2020-3439 CISCO
cisco -- data_center_network_manager	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of the affected software. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2020-08-26	3.5	CVE-2020-3518 CISCO
cisco -- data_center_network_manager	A vulnerability in Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, local attacker to obtain confidential information from an affected device. The vulnerability is due to insufficient protection of confidential information on an affected device. An attacker at any privilege level could exploit this vulnerability by accessing local filesystems and extracting sensitive information from them. A successful exploit could allow the attacker to view sensitive data, which they could use to elevate their privilege.	2020-08-26	2.1	CVE-2020-3520 CISCO
cookielawinfo -- gdpr_cookie_consent	ajax_policy_generator in admin/modules/cli-policy-generator/classes/class-policy-generator-ajax.php in GDPR Cookie Consent (cookie-law-info) 1.8.2 and below plugin for WordPress, allows authenticated stored XSS and privilege escalation.	2020-08-21	3.5	CVE-2020-20633 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function in dbhcms\mod\mod.domain.edit.php line 119.	2020-08-24	3.5	CVE-2020-19884 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored XSS vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_description']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	2020-08-24	3.5	CVE-2020-19887 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_name']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	2020-08-24	3.5	CVE-2020-19885 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter in dbhcms\mod\mod.users.view.php line 57 for user_login, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	2020-08-24	3.5	CVE-2020-19883 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for 'menu_description' variable in dbhcms\mod\mod.menus.edit.php line 83 and in dbhcms\mod\mod.menus.view.php line 111, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	2020-08-24	3.5	CVE-2020-19882 MISC
dbhcms_project -- dbhcms	DBHcms v1.2.0 has a reflected xss vulnerability as there is no security filter in dbhcms\mod\mod.selector.php line 108 for $_GET['return_name'] parameter, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	2020-08-24	3.5	CVE-2020-19881 MISC
dieboldnixdorf -- probase	Diebold Nixdorf ProCash 2100xe USB ATMs running Wincor Probase version 1.1.30 do not encrypt, authenticate, or verify the integrity of messages between the CCDM and the host computer, allowing an attacker with physical access to internal ATM components to commit deposit forgery by intercepting and modifying messages to the host computer, such as the amount and value of currency being deposited.	2020-08-21	2.1	CVE-2020-9062 MISC
exceedone -- exment	Cross-site scripting vulnerability in Exment prior to v3.6.0 allows remote authenticated attackers to inject arbitrary script or HTML via unspecified vectors.	2020-08-25	3.5	CVE-2020-5619 MISC MISC
exceedone -- exment	Cross-site scripting vulnerability in Exment prior to v3.6.0 allows remote authenticated attackers to inject arbitrary script or HTML via a specially crafted file.	2020-08-25	3.5	CVE-2020-5620 MISC MISC
huawei -- p30_firmware	HUAWEI P30 smartphones with Versions earlier than 10.1.0.123(C431E22R2P5),Versions earlier than 10.1.0.123(C432E22R2P5),Versions earlier than 10.1.0.126(C10E7R5P1),Versions earlier than 10.1.0.126(C185E4R7P1),Versions earlier than 10.1.0.126(C461E7R3P1),Versions earlier than 10.1.0.126(C605E19R1P3),Versions earlier than 10.1.0.126(C636E7R3P4),Versions earlier than 10.1.0.128(C635E3R2P4),Versions earlier than 10.1.0.160(C00E160R2P11),Versions earlier than 10.1.0.160(C01E160R2P11) have a denial of service vulnerability. In specific scenario, due to the improper resource management and memory leak of some feature, the attacker could exploit this vulnerability to cause the device reset.	2020-08-21	3.3	CVE-2020-9104 MISC
huawei -- p30_pro_firmware	HUAWEI P30 Pro smartphone with Versions earlier than 10.1.0.160(C00E160R2P8) has an integer overflow vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause integer overflow. This can compromise normal service.	2020-08-21	2.1	CVE-2020-9095 MISC
huawei -- p30_pro_firmware	HUAWEI P30 Pro smartphones with Versions earlier than 10.1.0.160(C00E160R2P8) have an out of bound read vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause out-of-bound read. This can compromise normal service.	2020-08-21	2.1	CVE-2020-9096 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- elastic_storage_server	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment or upgrade pertaining to xcat services. IBM X-Force ID: 179163.	2020-08-24	2.1	CVE-2020-4382 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 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: 171828.	2020-08-26	3.5	CVE-2019-4691 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 171926.	2020-08-26	2.1	CVE-2019-4695 XF CONFIRM
ibm -- guardium_data_encryption	IBM Security Guardium Data Encryption (GDE) 3.0.0.2 stores user credentials in plain in clear text which can be read by a local privileged user. IBM X-Force ID: 171831.	2020-08-26	2.1	CVE-2019-4693 XF CONFIRM
ibm -- security_guardium_insights	IBM Security Guardium Insights 2.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 184747.	2020-08-24	2.1	CVE-2020-4593 XF CONFIRM
mcafee -- total_protection	Privilege Escalation vulnerability in the installer in McAfee McAfee Total Protection (MTP) trial prior to 4.0.161.1 allows local users to change files that are part of write protection rules via manipulating symbolic links to redirect a McAfee file operations to an unintended file.	2020-08-21	3.3	CVE-2020-7310 CONFIRM
naviwebs -- navigatecms	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Configuration."	2020-08-26	3.5	CVE-2020-23657 MISC
naviwebs -- navigatecms	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Content."	2020-08-26	3.5	CVE-2020-23656 MISC
naviwebs -- navigatecms	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) via the module "Shop."	2020-08-26	3.5	CVE-2020-23654 MISC
naviwebs -- navigatecms	NavigateCMS 2.9 is affected by Cross Site Scripting (XSS) on module "Configuration."	2020-08-26	3.5	CVE-2020-23655 MISC
ncr -- aptra_xfs	The currency dispenser of NCR SelfSev ATMs running APTRA XFS 05.01.00 or earlier does not adequately authenticate session key generation requests from the host computer, allowing an attacker with physical access to internal ATM components to issue valid commands to dispense currency by generating a new session key that the attacker knows.	2020-08-21	2.1	CVE-2020-10123 MISC MISC MISC MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- nextcloud	A cross-site scripting error in Nextcloud Desktop client 2.6.4 allowed to present any html (including local links) when responding with invalid data on the login attempt.	2020-08-21	3.5	CVE-2020-8189 MISC MISC
osticket -- osticket	osTicket before 1.14.3 allows XSS because include/staff/banrule.inc.php has an unvalidated echo $info['notes'] call.	2020-08-26	3.5	CVE-2020-16193 MISC CONFIRM
parallels -- parallels_desktop	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.3-47255. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result a pointer to be leaked after the handler is done. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-10520.	2020-08-25	2.1	CVE-2020-17393 MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-11302.	2020-08-25	2.1	CVE-2020-17398 MISC MISC
parallels -- parallels_desktop	This vulnerability allows local attackers to disclose sensitive informations on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the VGA virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated array. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11363.	2020-08-25	2.1	CVE-2020-17401 MISC MISC
philips -- suresigns_vs4_firmware	Philips SureSigns VS4, A.07.107 and prior. The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.	2020-08-21	2.1	CVE-2020-16241 MISC
philips -- suresigns_vs4_firmware	Philips SureSigns VS4, A.07.107 and prior. The product receives input or data, but it does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly.	2020-08-21	2.1	CVE-2020-16237 MISC
tenable -- nessus	Nessus versions 8.11.0 and earlier were found to maintain sessions longer than the permitted period in certain scenarios. The lack of proper session expiration could allow attackers with local access to login into an existing browser session.	2020-08-21	3.6	CVE-2020-5774 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vmware -- app_volumes	VMware App Volumes 2.x prior to 2.18.6 and VMware App Volumes 4 prior to 2006 contain a Stored Cross-Site Scripting (XSS) vulnerability. A malicious actor with access to create and edit applications or create storage groups, may be able to inject malicious script which will be executed by a victim's browser when viewing.	2020-08-21	3.5	CVE-2020-3975 MISC
webport_project -- webport	WebPort-v1.19.17121 is affected by Cross Site Scripting (XSS) on the "connections" feature.	2020-08-26	3.5	CVE-2020-23659 MISC
webtareas_project -- webtareas	webTareas v2.1 is affected by Cross Site Scripting (XSS) on "Search."	2020-08-26	3.5	CVE-2020-23660 MISC