BULLETIN (SB20-216)
VULNERABILITY SUMMARY FOR THE WEEK OF 27TH JULY, 2020

Bulletin (SB20-216)
Vulnerability Summary for the Week of July 27, 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
adobe -- magento	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a path traversal vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-07-29	8.5	CVE-2020-9689 CONFIRM
adobe -- magento	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-07-29	8.5	CVE-2020-9692 CONFIRM
adobe -- magento	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a dom-based cross-site scripting vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-07-29	9.3	CVE-2020-9691 CONFIRM
arris -- ruckus_wireless_unleashed	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	7.5	CVE-2020-13917 CONFIRM
arris -- ruckus_wireless_unleashed	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	7.5	CVE-2020-13916 CONFIRM
arris -- ruckus_wireless_unleashed	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	7.5	CVE-2020-13919 CONFIRM
artifex_software -- ghostscript	A memory corruption issue was found in Artifex Ghostscript 9.50 and 9.52. Use of a non-standard PostScript operator can allow overriding of file access controls. The 'rsearch' calculation for the 'post' size resulted in a size that was too large, and could underflow to max uint32_t. This was fixed in commit 5d499272b95a6b890a1397e11d20937de000d31b.	2020-07-28	7.5	CVE-2020-15900 MISC CONFIRM MISC MISC MISC
aternity -- steelcentral_aternity_agent	SteelCentral Aternity Agent 11.0.0.120 on Windows mishandles IPC. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. Any user in the system is allowed to access the interprocess communication channel AternityAgentAssistantIpc, retrieve a serialized object and call object methods remotely. Among others, the methods allow any user to: (1) Create and/or overwrite arbitrary XML files across the system; (2) Create arbitrary directories across the system; and (3) Load arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)/Aternity Information Systems/Assistant/plugins” directory and execute code contained in them.	2020-07-27	7.2	CVE-2020-15593 CONFIRM MISC

control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_disk_usage.php. When parsing the folderName parameter, the process does not properly validate 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 root. Was ZDI-CAN-9713.	2020-07-28	10	CVE-2020-15427 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the username parameter, the process does not properly validate 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 root. Was ZDI-CAN-9736.	2020-07-28	10	CVE-2020-15430 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_new_account.php. When parsing the domain parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9727.	2020-07-28	7.8	CVE-2020-15624 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the search parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9712.	2020-07-28	7.8	CVE-2020-15622 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-el7-0.9.8.891. Authentication is not required to exploit this vulnerability. The specific flaw exists within loader_ajax.php. When parsing the line parameter, the process does not properly validate 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 root. Was ZDI-CAN-9259.	2020-07-28	10	CVE-2020-15420 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the line parameter, the process does not properly validate 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 root. Was ZDI-CAN-9714.	2020-07-28	10	CVE-2020-15428 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the user parameter, the process does not properly validate 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 root. Was ZDI-CAN-9716.	2020-07-28	10	CVE-2020-15429 N/A

control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the user parameter, the process does not properly validate 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 root. Was ZDI-CAN-9740.	2020-07-28	10	CVE-2020-15431 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the phpversion parameter, the process does not properly validate 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 root. Was ZDI-CAN-9715.	2020-07-28	10	CVE-2020-15433 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the canal parameter, the process does not properly validate 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 root. Was ZDI-CAN-9745.	2020-07-28	10	CVE-2020-15434 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_start parameter, the process does not properly validate 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 root. Was ZDI-CAN-9719.	2020-07-28	10	CVE-2020-15435 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the type parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9723.	2020-07-28	7.8	CVE-2020-15619 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the username parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9717.	2020-07-28	7.8	CVE-2020-15618 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the ai_service parameter, the process does not properly validate 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 root. Was ZDI-CAN-9724.	2020-07-28	10	CVE-2020-15608 N/A

control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_stop parameter, the process does not properly validate 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 root. Was ZDI-CAN-9726.	2020-07-28	10	CVE-2020-15609 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the modulo parameter, the process does not properly validate 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 root. Was ZDI-CAN-9728.	2020-07-28	10	CVE-2020-15610 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_restart parameter, the process does not properly validate 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 root. Was ZDI-CAN-9734.	2020-07-28	10	CVE-2020-15611 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. 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 root. Was ZDI-CAN-9742.	2020-07-28	10	CVE-2020-15425 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. 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 root. Was ZDI-CAN-9720.	2020-07-28	10	CVE-2020-15606 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_migration_cpanel.php. When parsing the serverip parameter, the process does not properly validate 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 root. Was ZDI-CAN-9709.	2020-07-28	10	CVE-2020-15426 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_ftp_manager.php. When parsing the userLogin parameter, the process does not properly validate 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 root. Was ZDI-CAN-9737.	2020-07-28	10	CVE-2020-15612 N/A

control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. When parsing the line parameter, the process does not properly validate 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 root. Was ZDI-CAN-9721.	2020-07-28	10	CVE-2020-15607 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the user parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9710.	2020-07-28	7.8	CVE-2020-15628 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the archivo parameter, the process does not properly validate 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 root. Was ZDI-CAN-9731.	2020-07-28	10	CVE-2020-15422 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_ftp_manager.php. 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 root. Was ZDI-CAN-9746.	2020-07-28	10	CVE-2020-15615 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the check_ip parameter, the process does not properly validate 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 root. Was ZDI-CAN-9707.	2020-07-28	10	CVE-2020-15421 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the email parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9711.	2020-07-28	7.8	CVE-2020-15621 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_add_mailbox.php. When parsing the username parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9729.	2020-07-28	7.8	CVE-2020-15625 N/A

control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the id parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9741.	2020-07-28	7.8	CVE-2020-15620 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the term parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9730.	2020-07-28	7.8	CVE-2020-15626 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the account parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9738.	2020-07-28	7.8	CVE-2020-15627 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the status parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9708.	2020-07-28	7.8	CVE-2020-15617 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to write arbitrary files on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the archivo parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9722.	2020-07-28	10	CVE-2020-15623 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. When parsing the line parameter, the process does not properly validate 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 root. Was ZDI-CAN-9739.	2020-07-28	10	CVE-2020-15613 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the cha parameter, the process does not properly validate 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 root. Was ZDI-CAN-9718.	2020-07-28	10	CVE-2020-15614 N/A

control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_migration_cpanel.php. When parsing the filespace parameter, the process does not properly validate 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 root. Was ZDI-CAN-9743.	2020-07-28	10	CVE-2020-15432 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the domain parameter, the process does not properly validate 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 root. Was ZDI-CAN-9735.	2020-07-28	10	CVE-2020-15424 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the dominio parameter, the process does not properly validate 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 root. Was ZDI-CAN-9732.	2020-07-28	10	CVE-2020-15423 N/A
control_web_panel -- centos_web_panel	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the package parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9706.	2020-07-28	7.8	CVE-2020-15616 N/A
fortinet -- fortios	An improper authentication vulnerability in SSL VPN in FortiOS 6.4.0, 6.2.0 to 6.2.3, 6.0.9 and below may result in a user being able to log in successfully without being prompted for the second factor of authentication (FortiToken) if they changed the case of their username.	2020-07-24	7.5	CVE-2020-12812 MISC
gerapy -- gerapy	This affects the package Gerapy from 0 and before 0.9.3. The input being passed to Popen, via the project_configure endpoint, isn't being sanitized.	2020-07-29	7.5	CVE-2020-7698 MISC MISC
grandstream -- ht800_series_devices	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt.	2020-07-29	9	CVE-2020-5763 MISC MISC
grandstream -- ht800_series_devices	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service.	2020-07-29	7.8	CVE-2020-5761 MISC MISC
grandstream -- ht800_series_devices	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message.	2020-07-29	9.3	CVE-2020-5760 MISC MISC

libssh -- libssh	libssh 0.9.4 has a NULL pointer dereference in tftpserver.c if ssh_buffer_new returns NULL.	2020-07-29	7.5	CVE-2020-16135 MISC MISC MISC MLIST
mida_solutions -- eframework	Mida eFramework through 2.9.0 allows unauthenticated ../ directory traversal.	2020-07-24	7.8	CVE-2020-15923 MISC
mida_solutions -- eframework	Mida eFramework through 2.9.0 has a back door that permits a change of the administrative password and access to restricted functionalities, such as Code Execution.	2020-07-24	7.5	CVE-2020-15921 MISC
mida_solutions -- eframework	There is an OS Command Injection in Mida eFramework 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. Authentication is required.	2020-07-24	10	CVE-2020-15922 MISC
mida_solutions -- eframework	There is an OS Command Injection in Mida eFramework through 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. No authentication is required.	2020-07-24	10	CVE-2020-15920 MISC
mock2easy -- mock2easy	This affects all versions of package mock2easy. a malicious user could inject commands through the _data variable: Affected Area require('../server/getJsonByCurl')(mock2easy, function (error, stdout) { if (error) { return res.json(500, error); } res.json(JSON.parse(stdout)); }, '', _data.interfaceUrl, query, _data.cookie,_data.interfaceType);	2020-07-29	7.5	CVE-2020-7697 MISC MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9703.	2020-07-28	8.3	CVE-2020-15416 MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPnP service, which listens on TCP port 5000. A crafted UPnP message can be used to bypass authentication. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9642.	2020-07-28	8.3	CVE-2020-10923 MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to compromise the integrity of downloaded information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloading of files via HTTPS. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9647.	2020-07-28	8.3	CVE-2020-10925 MISC

netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the encryption of firmware update images. The issue results from the use of an inappropriate encryption algorithm. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9649.	2020-07-28	8.3	CVE-2020-10927 MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of firmware updates. The issue results from the lack of proper validation of the firmware image prior to performing an upgrade. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9648.	2020-07-28	8.3	CVE-2020-10926 MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the UPnP service, which listens on TCP port 5000 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9643.	2020-07-28	8.3	CVE-2020-10924 MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. 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 execute code in the context of the admin user. Was ZDI-CAN-9768.	2020-07-28	8.3	CVE-2020-10929 MISC
node.js -- node.js	napi_get_value_string_*() allows various kinds of memory corruption in node < 10.21.0, 12.18.0, and < 14.4.0.	2020-07-24	10	CVE-2020-8174 MISC
openbsd_project -- openbsd	iked in OpenIKED, as used in OpenBSD through 6.7, allows authentication bypass because ca.c has the wrong logic for checking whether a public key matches.	2020-07-28	7.5	CVE-2020-16088 CONFIRM MISC MISC MISC
openclinic_ga -- openclinic_ga	OpenClinic GA 5.09.02 and 5.89.05b does not properly verify uploaded files, which may allow a low-privilege user to upload and execute arbitrary files on the system.	2020-07-29	9	CVE-2020-14488 MISC
openclinic_ga -- openclinic_ga	OpenClinic GA 5.09.02 contains a hidden default user account that may be accessed if an administrator has not expressly turned off this account, which may allow an attacker to login and execute arbitrary commands.	2020-07-29	7.5	CVE-2020-14487 MISC
opendmarc -- opendmarc	OpenDMARC through 1.3.2 and 1.4.x through 1.4.0-Beta1 has improper null termination in the function opendmarc_xml_parse that can result in a one-byte heap overflow in opendmarc_xml when parsing a specially crafted DMARC aggregate report. This can cause remote memory corruption when a '\0' byte overwrites the heap metadata of the next chunk and its PREV_INUSE flag.	2020-07-27	7.5	CVE-2020-12460 MISC MISC

portland_labs -- concrete5	Concrete5 before 8.5.3 allows Unrestricted Upload of File with Dangerous Type such as a .phar file.	2020-07-28	9	CVE-2020-11476 CONFIRM CONFIRM MISC MISC
pulse_secure -- pulse_connect_secure	An improper authentication vulnerability exists in Pulse Connect Secure <9.1RB that allows an attacker with a users primary credentials to bypass the Google TOTP.	2020-07-30	7.5	CVE-2020-8206 MISC
qemu -- qemu	hw/net/xgmac.c in the XGMAC Ethernet controller in QEMU before 07-20-2020 has a buffer overflow. This occurs during packet transmission and affects the highbank and midway emulated machines. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service or potential privileged code execution. This was fixed in commit 5519724a13664b43e225ca05351c60b4468e4555.	2020-07-28	7.2	CVE-2020-15863 CONFIRM CONFIRM MISC MISC
qualcomm -- multiple_snapdragon_products	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-07-30	7.5	CVE-2020-3699 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130	2020-07-30	7.5	CVE-2020-3698 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-07-30	7.5	CVE-2020-3688 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130	2020-07-30	7.5	CVE-2020-3671 CONFIRM MISC

zoho -- manageengine_desktop_central	An issue was discovered in the client side of Zoho ManageEngine Desktop Central before 10.0.533. An attacker-controlled server can trigger an integer overflow via a crafted header value.	2020-07-29	7.5	CVE-2020-15588 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arris -- ruckus_wireless_unleashed	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	5	CVE-2020-13914 CONFIRM
arris -- ruckus_wireless_unleashed	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	4.3	CVE-2020-13913 CONFIRM
arris -- ruckus_wireless_unleashed	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	5	CVE-2020-13918 CONFIRM
arris -- ruckus_wireless_unleashed	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	2020-07-28	6.4	CVE-2020-13915 CONFIRM
cherokee -- cherokee	Cherokee 0.4.27 to 1.2.104 is affected by a denial of service due to a NULL pointer dereferences. A remote unauthenticated attacker can crash the server by sending an HTTP request to protected resources using a malformed Authorization header that is mishandled during a cherokee_buffer_add call within cherokee_validator_parse_basic or cherokee_validator_parse_digest.	2020-07-27	5	CVE-2020-12845 MISC MISC MISC
citrix -- workspace	Improper access control in Citrix Workspace app for Windows 1912 CU1 and 2006.1 causes privilege escalation and code execution when the automatic updater service is running.	2020-07-24	6	CVE-2020-8207 MISC
elastic -- kibana	Kibana versions before 6.8.11 and 7.8.1 contain a denial of service (DoS) flaw in Timelion. An attacker can construct a URL that when viewed by a Kibana user can lead to the Kibana process consuming large amounts of CPU and becoming unresponsive.	2020-07-27	4.3	CVE-2020-7016 N/A N/A
fast-http -- fast-http	This affects all versions of package fast-http. There is no path sanitization in the path provided at fs.readFile in index.js.	2020-07-25	5	CVE-2020-7687 MISC
freediameter -- freediameter	An exploitable denial of service vulnerability exists in the freeDiameter functionality of freeDiameter 1.3.2. A specially crafted Diameter request can trigger a memory corruption resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	2020-07-28	5	CVE-2020-6098 MISC
gambio -- gx	Gambio GX before 4.0.1.0 allows admin/admin.php CSRF.	2020-07-28	6.8	CVE-2020-10984 MISC MISC
gambio -- gx	Gambio GX before 4.0.1.0 allows SQL Injection in admin/gv_mail.php.	2020-07-28	4	CVE-2020-10982 MISC MISC
gambio -- gx	Gambio GX before 4.0.1.0 allows SQL Injection in admin/mobile.php.	2020-07-28	4	CVE-2020-10983 MISC MISC
gnome -- balsa	In GNOME Balsa before 2.6.0, a malicious server operator or man in the middle can trigger a NULL pointer dereference and client crash by sending a PREAUTH response to imap_mbox_connect in libbalsa/imap/imap-handle.c.	2020-07-29	5	CVE-2020-16118 MISC MISC
gnome -- evolution-data-server	In GNOME evolution-data-server before 3.35.91, a malicious server can crash the mail client with a NULL pointer dereference by sending an invalid (e.g., minimal) CAPABILITY line on a connection attempt. This is related to imapx_free_capability and imapx_connect_to_server.	2020-07-29	5	CVE-2020-16117 MISC MISC MISC MLIST

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
grafana -- grafana	Grafana through 6.7.1 allows stored XSS due to insufficient input protection in the originalUrl field, which allows an attacker to inject JavaScript code that will be executed after clicking on Open Original Dashboard after visiting the snapshot.	2020-07-27	4.3	CVE-2020-11110 MISC
grandstream -- ht800_firmware	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field.	2020-07-29	5	CVE-2020-5762 MISC MISC
grundfos -- cim	Grundfos CIM 500 v06.16.00 stores plaintext credentials, which may allow sensitive information to be read or allow modification to system settings by someone with access to the device.	2020-07-27	5	CVE-2020-10609 CONFIRM
hmtalk -- daviewindy	DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2020-07-30	6.8	CVE-2020-7828 MISC
hmtalk -- daviewindy	DaviewIndy 8.98.7 and earlier version contain Use-After-Free vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2020-07-30	6.8	CVE-2020-7827 MISC
hmtalk -- daviewindy	DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2020-07-30	6.8	CVE-2020-7829 MISC
huawei -- p30_smartphones	HUAWEI P30 smart phones with versions earlier than 10.1.0.160(C00E160R2P11) have an information exposure vulnerability. The system does not properly authenticate the application that access a specified interface. Attackers can trick users into installing malicious software to exploit this vulnerability and obtain some information about the device. Successful exploit may cause information disclosure.	2020-07-27	4.3	CVE-2020-9077 MISC
i_hate_money -- i_hate_money	In "I hate money" before version 4.1.5, an authenticated member of one project can modify and delete members of another project, without knowledge of this other project's private code. This can be further exploited to access all bills of another project without knowledge of this other project's private code. With the default configuration, anybody is allowed to create a new project. An attacker can create a new project and then use it to become authenticated and exploit this flaw. As such, the exposure is similar to an unauthenticated attack, because it is trivial to become authenticated. This is fixed in version 4.1.5.	2020-07-27	4	CVE-2020-15120 MISC CONFIRM
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6.0.1 and 7.6.0.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 181484.	2020-07-29	6.4	CVE-2020-4463 XF CONFIRM
ibm -- mq_appliance	IBM MQ, IBM MQ Appliance, and IBM MQ for HPE NonStop 8.0, 9.1 CD, and 9.1 LTS is vulnerable to a buffer overflow vulnerability due to an error within the channel processing code. A remote attacker could overflow the buffer using an older client and cause a denial of service. IBM X-Force ID: 181562.	2020-07-28	4	CVE-2020-4465 XF CONFIRM
ibm -- mq_appliance	IBM MQ, IBM MQ Appliance, IBM MQ for HPE NonStop 8.0, 9.1 CD, and 9.1 LTS could allow an attacker to cause a denial of service due to a memory leak caused by an error creating a dynamic queue. IBM X-Force ID: 179080.	2020-07-28	5	CVE-2020-4375 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics Local 2.0.0 through 2.0.9.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 185716.	2020-07-29	5.8	CVE-2020-4644 XF CONFIRM
ibm -- tivoli_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 could disclose sensitive information due to responding to unauthenticated HTTP requests. IBM X-Force ID: 184180.	2020-07-29	5	CVE-2020-4573 XF CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- tivoli_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 184156.	2020-07-29	5	CVE-2020-4567 XF CONFIRM
ibm -- tivoli_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 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: 184179.	2020-07-29	5	CVE-2020-4572 XF CONFIRM
ibm -- tivoli_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 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: 184181.	2020-07-29	5	CVE-2020-4574 XF CONFIRM
ibm -- tivoli_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted actor in a way that bypasses the protection mechanism. IBM X-Force ID: 184158.	2020-07-29	6.4	CVE-2020-4569 XF CONFIRM
ibm -- verify_gateway	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 could disclose potentially sensitive information to an authenticated user due to world readable log files. IBM X-Force ID: 179484.	2020-07-27	4	CVE-2020-4405 XF CONFIRM
jpeg-js -- jpeg-js	Uncontrolled resource consumption in `jpeg-js` before 0.4.0 may allow attacker to launch denial of service attacks using specially a crafted JPEG image.	2020-07-24	4.3	CVE-2020-8175 MISC
kde -- kmail	KDE KMail 19.12.3 (aka 5.13.3) engages in unencrypted POP3 communication during times when the UI indicates that encryption is in use.	2020-07-27	4.3	CVE-2020-15954 MISC MLIST
konawiki -- konawiki	Cross-site scripting vulnerability in KonaWiki 3.1.0 and earlier allows remote attackers to execute an arbitrary script via a specially crafted URL.	2020-07-29	4.3	CVE-2020-5613 MISC MISC
konawiki -- konawiki	Cross-site scripting vulnerability in KonaWiki 2.2.0 and earlier allows remote attackers to execute an arbitrary script via a specially crafted URL.	2020-07-29	4.3	CVE-2020-5612 MISC MISC
konawiki -- konawiki	Directory traversal vulnerability in KonaWiki 3.1.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors.	2020-07-29	5	CVE-2020-5614 MISC MISC
kubernetes -- kubernetes	The Kubelet and kube-proxy components in versions 1.1.0-1.16.10, 1.17.0-1.17.6, and 1.18.0-1.18.3 were found to contain a security issue which allows adjacent hosts to reach TCP and UDP services bound to 127.0.0.1 running on the node or in the node's network namespace. Such a service is generally thought to be reachable only by other processes on the same host, but due to this defeect, could be reachable by other hosts on the same LAN as the node, or by containers running on the same node as the service.	2020-07-27	5.8	CVE-2020-8558 CONFIRM MLIST
lenovo -- drivers_management	An unquoted service path vulnerability was reported in Lenovo Drivers Management prior to version 2.7.1128.1046 that could allow an authenticated user to execute code with elevated privileges.	2020-07-24	6.9	CVE-2020-8326 CONFIRM
lenovo -- drivers_management	A DLL search path vulnerability was reported in Lenovo Drivers Management prior to version 2.7.1128.1046 that could allow an authenticated user to execute code with elevated privileges.	2020-07-24	6.9	CVE-2020-8317 CONFIRM
libetpan -- mailcore	LibEtPan through 1.9.4, as used in MailCore 2 through 0.6.3 and other products, has a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a meddler-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection."	2020-07-27	5.8	CVE-2020-15953 MISC GENTOO
lua -- lua	Lua through 5.4.0 has a segmentation fault in changedline in ldebug.c (e.g., when called by luaG_traceexec) because it incorrectly expects that an oldpc value is always updated upon a return of the flow of control to a function.	2020-07-24	5	CVE-2020-15945 MISC MISC
marked-tree -- marked-tree	This affects all versions of package marked-tree. There is no path sanitization in the path provided at fs.readFile in index.js.	2020-07-25	5	CVE-2020-7682 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
marscode -- marscode	This affects all versions of package marscode. There is no path sanitization in the path provided at fs.readFile in index.js.	2020-07-25	5	CVE-2020-7681 MISC
microsoft -- windows_codecs_library	A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1457.	2020-07-27	6.8	CVE-2020-1425 MISC
microsoft -- windows_codecs_library	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1425.	2020-07-27	6.8	CVE-2020-1457 MISC
mida -- eframework	There is a SQL Injection in Mida eFramework through 2.9.0 that leads to Information Disclosure. No authentication is required. The injection point resides in one of the authentication parameters.	2020-07-24	5	CVE-2020-15924 MISC
mida -- eframework	A Reflected Cross Site Scripting (XSS) vulnerability was discovered in Mida eFramework through 2.9.0.	2020-07-24	4.3	CVE-2020-15919 MISC
ncp -- secure_enterprise_client	NCP Secure Enterprise Client before 10.15 r47589 allows a symbolic link attack on enumusb.reg via Support Assistant.	2020-07-28	4.6	CVE-2020-11474 MISC MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9767.	2020-07-28	4.6	CVE-2020-10928 MISC
netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. A crafted gui_region in a string table file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9756.	2020-07-28	5.8	CVE-2020-15417 MISC
openbsd -- openssh	scp in OpenSSH through 8.3p1 allows command injection in scp.c remote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."	2020-07-24	6.8	CVE-2020-15778 MISC CONFIRM MISC
openclinic_ga -- openclinic_ga	OpenClinic GA 5.09.02 and 5.89.05b includes arbitrary local files specified within its parameter and executes some files, which may allow disclosure of sensitive files or the execution of malicious uploaded files.	2020-07-29	6.5	CVE-2020-14490 MISC
openclinic_ga -- openclinic_ga	A low-privilege user may use SQL syntax to write arbitrary files to the OpenClinic GA 5.09.02 and 5.89.05b server, which may allow the execution of arbitrary commands.	2020-07-29	6.5	CVE-2020-14493 MISC
openclinic_ga -- openclinic_ga	OpenClinic GA 5.09.02 and 5.89.05b stores passwords using inadequate hashing complexity, which may allow an attacker to recover passwords using known password cracking techniques.	2020-07-29	5	CVE-2020-14489 MISC
openclinic_ga -- openclinic_ga	OpenClinic GA 5.09.02 and 5.89.05b does not properly neutralize user-controllable input, which may allow the execution of malicious code within the user's browser.	2020-07-29	4.3	CVE-2020-14492 MISC
openclinic_ga -- openclinic_ga	An attacker may bypass permission/authorization checks in OpenClinic GA 5.09.02 and 5.89.05b by ignoring the redirect of a permission failure, which may allow unauthorized execution of commands.	2020-07-29	6.5	CVE-2020-14486 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network	2020-07-24	4	CVE-2020-14725 CONFIRM MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).			
parallels -- remote_application_server	Parallels Remote Application Server (RAS) 17.1.1 has a Business Logic Error causing remote code execution. It allows an authenticated user to execute any application in the backend operating system through the web application, despite the affected application not being published. In addition, it was discovered that it is possible to access any host in the internal domain, even if it has no published applications or the mentioned host is no longer associated with that server farm.	2020-07-24	6.5	CVE-2020-15860 MISC MISC
pulse_secure -- pulse_connect_secure	A cross site scripting (XSS) vulnerability exists in Pulse Connect Secure <9.1R5 on the PSAL Page.	2020-07-30	4.3	CVE-2020-8204 MISC
pulse_secure -- pulse_connect_secure	An information disclosure vulnerability in meeting of Pulse Connect Secure <9.1R8 allowed an authenticated end-users to find meeting details, if they know the Meeting ID.	2020-07-30	4	CVE-2020-8216 MISC
pulse_secure -- pulse_connect_secure	An issue was discovered in Pulse Secure Pulse Connect Secure before 9.1R8. An authenticated attacker can access the admin page console via the end-user web interface because of a rewrite.	2020-07-28	5.8	CVE-2020-15408 MISC CONFIRM
pulse_secure -- pulse_connect_secure	A code injection vulnerability exists in Pulse Connect Secure <9.1RB that allows an attacker to crafted a URI to perform an arbitrary code execution via the admin web interface.	2020-07-30	6.5	CVE-2020-8218 MISC
qualcomm -- multiple_snapdragon_products	Memory corruption can occurs in trusted application if offset size from HLOS is more than actual mapped buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	2020-07-30	4.6	CVE-2019-14130 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Close and bind operations done on a socket can lead to a Use-After-Free condition. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8996, MSM8996AU, QCN7605, QCN7606, QCS605, SC8180X, SDA660, SDA845, SDM439, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-07-30	4.6	CVE-2019-14037 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Register write via debugfs is disabled by default to prevent register writing via debugfs. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9206, MDM9207C, MDM9607, Nicobar, QCS405, SA6155P, SC8180X, SDX55, SM8150	2020-07-30	4.6	CVE-2019-14100 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Possible buffer overflow and over read possible due to missing bounds checks for fixed limits if we consider widevine HLOS client as non-trustable in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	2020-07-30	4.6	CVE-2019-14123 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Device misbehavior may be observed when incorrect offset, length or number of buffers is passed by user space in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, Nicobar, QCM2150, QCS405, QCS605, QM215, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-07-30	4.6	CVE-2019-14099 CONFIRM MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- multiple_snapdragon_products	When kernel thread unregistered listener, Use after free issue happened as the listener client`s private data has been already freed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MSM8909W, Nicobar, QCM2150, QCS405, QCS605, Saipan, SC8180X, SDM429W, SDX55, SM8150, SM8250, SXR2130	2020-07-30	4.6	CVE-2019-10580 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Memory failure in content protection module due to not having pointer within the scope in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, QCS404, Rennell, SC7180, SDX55, SM6150, SM7150, SM8250, SXR2130	2020-07-30	4.6	CVE-2019-14124 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Array out of bound access can occur in display module due to lack of bound check on input parcel received in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCM2150, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM636, SDM660, SDX20	2020-07-30	4.6	CVE-2019-14093 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130	2020-07-30	4.6	CVE-2020-3701 CONFIRM MISC
qualcomm -- multiple_snapdragon_products	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130	2020-07-30	5	CVE-2020-3700 CONFIRM MISC
rconfig -- rconfig	rConfig 3.9.5 could allow a remote authenticated attacker to execute arbitrary code on the system, because of an error in the search.crud.php script. An attacker could exploit this vulnerability using the nodeId parameter.	2020-07-28	6.5	CVE-2020-15715 MISC MISC
rconfig -- rconfig	rConfig 3.9.5 is vulnerable to SQL injection. A remote authenticated attacker could send crafted SQL statements to the devices.crud.php script using the custom_Location parameter, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2020-07-28	6.5	CVE-2020-15714 MISC MISC
rconfig -- rconfig	rConfig 3.9.5 is vulnerable to SQL injection. A remote authenticated attacker could send crafted SQL statements to the devices.php script using the sortBy parameter, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2020-07-28	6.5	CVE-2020-15713 MISC MISC
rconfig -- rconfig	rConfig 3.9.5 could allow a remote authenticated attacker to traverse directories on the system. An attacker could send a crafted request to the ajaxGetFileByPath.php script containing hexadecimal encoded "dot dot" sequences (%2f..%2f) in the path parameter to view arbitrary files on the system.	2020-07-28	4	CVE-2020-15712 MISC MISC
rollup-plugin-server -- rollup-plugin-server	This affects all versions of package rollup-plugin-dev-server. There is no path sanitization in readFile operation inside the readFileFromContentBase function.	2020-07-25	5	CVE-2020-7686 MISC
rollup-plugin-server -- rollup-plugin-server	This affects all versions of package rollup-plugin-server. There is no path sanitization in readFile operation performed inside the readFileFromContentBase function.	2020-07-25	5	CVE-2020-7683 MISC
shopware -- shopware	Shopware before 6.2.3 is vulnerable to a Server-Side Request Forgery (SSRF) in its "Mediabrowser upload by URL" feature. This allows an authenticated user to send HTTP, HTTPS, FTP, and SFTP requests on behalf of the Shopware platform server.	2020-07-28	6.5	CVE-2020-13970 CONFIRM CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
shopware -- shopware	In Shopware before 6.2.3, the database password is leaked to an unauthenticated user when a DriverException occurs and verbose error handling is enabled.	2020-07-28	5	CVE-2020-13997 CONFIRM CONFIRM
steelcentral -- aternity_agent	SteelCentral Aternity Agent before 11.0.0.120 on Windows allows Privilege Escalation via a crafted file. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. The remotely callable methods from remotable objects available through interprocess communication allow loading of arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)%/Aternity Information Systems/Assistant/plugins” directory, where the name of the plugin is passed as part of an XML-serialized object. However, because the name of the DLL is concatenated with the “.\plugins” string, a directory traversal vulnerability exists in the way plugins are resolved.	2020-07-27	5	CVE-2020-15592 CONFIRM MISC
typo3 -- kitodo_presentation	The dlf (aka Kitodo.Presentation) extension before 3.1.2 for TYPO3 allows XSS.	2020-07-29	4.3	CVE-2020-16095 MISC CONFIRM
umbracoforms -- umbracoforms	This affects all versions of package UmbracoForms. When using the default configuration for upload forms, it is possible to upload arbitrary file types. The package offers a way for users to mitigate the issue. The users of this package can create a custom workflow and frontend validation that blocks certain file types, depending on their security needs and policies.	2020-07-28	5	CVE-2020-7685 CONFIRM
uvicorn -- uvicorn	Uvicorn before 0.11.7 is vulnerable to HTTP response splitting. CRLF sequences are not escaped in the value of HTTP headers. Attackers can exploit this to add arbitrary headers to HTTP responses, or even return an arbitrary response body, whenever crafted input is used to construct HTTP headers.	2020-07-27	5	CVE-2020-7695 MISC MISC
wildfly -- enterprise_java_beans_client	A flaw was discovered in Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and cause denial of service attack and make services unavailable.	2020-07-24	4	CVE-2020-14297 CONFIRM
wildfly -- enterprise_java_beans_client	A vulnerability was found in Wildfly's Enterprise Java Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable.	2020-07-24	4	CVE-2020-14307 CONFIRM
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Social Sharing Plugin versions prior to 1.2.10 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2020-07-27	6.8	CVE-2020-5611 MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- magento	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass.	2020-07-29	3.5	CVE-2020-9690 CONFIRM
atlassian -- confluence_server_and_data_center	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in user macro parameters. The affected versions are before version 7.4.2, and from version 7.5.0 before 7.5.2.	2020-07-24	3.5	CVE-2020-14175 N/A
elastic -- kibana	In Kibana versions before 6.8.11 and 7.8.1 the region map visualization in contains a stored XSS flaw. An attacker who is able to edit or create a region map visualization could obtain sensitive information or perform destructive actions on behalf of Kibana users who view the region map visualization.	2020-07-27	3.5	CVE-2020-7017 N/A N/A
freerdp -- freerdp	In FreeRDP less than or equal to 2.1.2, an integer overflow exists due to missing input sanitation in rdpegfx channel. All FreeRDP clients are affected. The input rectangles from the server are not checked against local surface coordinates and blindly accepted. A malicious server can send data that will crash the client later on (invalid length arguments to a `memcpy`) This has been fixed in 2.2.0. As a workaround, stop using command line arguments /gfx, /gfx-h264 and /network:auto	2020-07-27	3.5	CVE-2020-15103 MISC MISC CONFIRM FEDORA FEDORA
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.1.0.160(C00E160R2P11) have an improper authorization vulnerability. The software does not properly restrict certain operation in certain scenario, the attacker should do certain configuration before the user turns on student mode function. Successful exploit could allow the attacker to bypass the limit of student mode function. Affected product versions include: HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8).	2020-07-27	2.1	CVE-2020-9251 MISC
ibm -- mq_appliance	IBM MQ Appliance 9.1 LTS and 9.1 CD could allow a local privileged user to obtain highly sensitve information due to inclusion of data within trace files. IBM X-Force ID: 182118.	2020-07-27	2.1	CVE-2020-4498 XF CONFIRM
ibm -- mq_appliance	IBM MQ Appliance 9.1.4.CD could allow a local attacker to obtain highly sensitive information by inclusion of sensitive data within trace. IBM X-Force ID: 172616.	2020-07-28	2.1	CVE-2019-4731 XF CONFIRM
ibm -- multiple_products	IBM MQ, IBM MQ Appliance, and IBM MQ for HPE NonStop 8.0, 9.1 LTS, and 9.1 CD could allow under special circumstances, an authenticated user to obtain sensitive information due to a data leak from an error message within the pre-v7 pubsub logic. IBM X-Force ID: 177402.	2020-07-28	3.5	CVE-2020-4319 XF CONFIRM
ibm -- multiple_products	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are 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: 177356.	2020-07-28	3.5	CVE-2020-4318 XF CONFIRM
ibm -- multiple_products	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are 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: 177355.	2020-07-28	3.5	CVE-2020-4317 XF CONFIRM
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0.0 through 2.0.9.1 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: 185717.	2020-07-29	3.5	CVE-2020-4645 XF CONFIRM
ibm -- qradar_advisor	The IBM QRadar Advisor 1.1 through 2.5.2 with Watson App for IBM QRadar SIEM does not adequately mask all passwords during input, which could be obtained by a physical attacker nearby. IBM X-Force ID: 179536.	2020-07-27	2.1	CVE-2020-4408 XF CONFIRM
mida_solutions -- eframework	Multiple Stored Cross Site Scripting (XSS) vulnerabilities were discovered in Mida eFramework through 2.9.0.	2020-07-24	3.5	CVE-2020-15918 MISC

netgear -- r6700_routers	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of URLs. The issue results from the lack of proper routing of URLs. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-9618.	2020-07-28	3.3	CVE-2020-10930 MISC
pulse_secure -- pulse_connect_secure	A cross site scripting (XSS) vulnerability in Pulse Connect Secure <9.1R8 allowed attackers to exploit in the URL used for Citrix ICA.	2020-07-30	3.5	CVE-2020-8217 MISC
pulse_secure -- pulse_policy_secure_and_pulse_connect_secure_virtual_appliance	An issue was discovered in Pulse Policy Secure (PPS) and Pulse Connect Secure (PCS) Virtual Appliance before 9.1R8. By manipulating a certain kernel boot parameter, it can be tricked into dropping into a root shell in a pre-install phase where the entire source code of the appliance is available and can be retrieved. (The source code is otherwise inaccessible because the appliance has its hard disks encrypted, and no root shell is available during normal operation.)	2020-07-27	2.1	CVE-2020-12880 MISC CONFIRM
qualcomm -- multiple_snapdragon_products	Out of bounds read can happen in diag event set mask command handler when user provided length in the command request is less than expected length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCN7605, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2020-07-30	3.6	CVE-2019-14101 CONFIRM MISC
shopware -- shopware	In Shopware before 6.2.3, authenticated users are allowed to use the Mediabrowser fileupload feature to upload SVG images containing JavaScript. This leads to Persistent XSS. An uploaded image can be accessed without authentication.	2020-07-28	3.5	CVE-2020-13971 CONFIRM CONFIRM
usd_herolab -- gambio_gx	Gambio GX before 4.0.1.0 allows XSS in admin/coupon_admin.php.	2020-07-28	3.5	CVE-2020-10985 MISC MISC