BULLETIN (SB20-125)
VULNERABILITY SUMMARY FOR THE WEEK OF
APRIL 27, 2020

Bulletin (SB20-125)
Vulnerability Summary for the Week of April 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
atrifex -- jbig2dec	jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow.	2020-04-27	7.5	CVE-2020-12268 MISC MISC MISC
canonical -- ubuntu	Overlayfs in the Linux kernel and shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patchs change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount underflow.	2020-04-24	7.2	CVE-2019-15794 MISC MISC MISC MISC
f5 -- big-iq	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	2020-04-24	10	CVE-2020-5868 MISC
google -- openthread	OpenThread before 2019-12-13 has a stack-based buffer overflow in MeshCoP::Commissioner::GeneratePskc.	2020-04-28	7.5	CVE-2019-20791 MISC MISC MISC
huawei -- ar3200_products	Huawei AR3200 products with versions of V200R007C00SPC900, V200R007C00SPCa00, V200R007C00SPCb00, V200R007C00SPCc00, V200R009C00SPC500 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device.	2020-04-27	7.5	CVE-2020-9068 CONFIRM
ivanti -- avalanche	Ivanti Avalanche 6.3 allows a SQL injection that is vaguely associated with the Apache HTTP Server, aka Bug 683250.	2020-04-28	7.5	CVE-2020-12442 MISC
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code>, controlling the redirect_uri, and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	2020-04-24	7.5	CVE-2020-6823 MISC MISC
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	2020-04-24	7.5	CVE-2020-6826 MISC MISC
mozilla -- multiple_products	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of	2020-04-24	7.5	CVE-2020-6825 MISC UBUNTU

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.			MISC MISC MISC
netgear -- wnr854t_devices	NETGEAR WNR854T devices before 1.5.2 are affected by command execution.	2020-04-29	8.3	CVE-2017-18855 CONFIRM
node-rules -- node-rules	node-rules including 3.0.0 and prior to 5.0.0 allows injection of arbitrary commands. The argument rules of function "fromJSON()" can be controlled by users without any sanitization.	2020-04-27	7.5	CVE-2020-7609 MISC MISC MISC
pixlcore -- pixl-class	pixl-class prior to 1.0.3 allows execution of arbitrary commands. The members argument of the create function can be controlled by users without any sanitization.	2020-04-27	7.5	CVE-2020-7640 MISC MISC MISC
qt -- qt	setMarkdown in Qt before 5.14.2 has a use-after-free related to QTextMarkdownImporter::insertBlock.	2020-04-27	7.5	CVE-2020-12267 MISC CONFIRM
shareit -- shareit	SHAREit through 4.0.6.177 does not check the body length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation.	2020-04-27	7.8	CVE-2019-14941 MISC MISC
shareit -- shareit	SHAREit through 4.0.6.177 does not check the full message length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation. This is different from CVE-2019-14941.	2020-04-27	7.8	CVE-2019-15234 MISC MISC
sophos -- xg_firewall_devices	A SQL injection issue was found in SFOS 17.0, 17.1, 17.5, and 18.0 before 2020-04-25 on Sophos XG Firewall devices, as exploited in the wild in April 2020. This affected devices configured with either the administration (HTTPS) service or the User Portal exposed on the WAN zone. A successful attack may have caused remote code execution that exfiltrated usernames and hashed passwords for the local device admin(s), portal admins, and user accounts used for remote access (but not external Active Directory or LDAP passwords)	2020-04-27	7.5	CVE-2020-12271 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abbs -- software_audio_media_player	ABBS Software Audio Media Player version 3.1 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	6.8	CVE-2019-5621 MISC
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	2020-04-24	5	CVE-2020-11004 MISC MISC CONFIRM
apache -- ats	Apache ATS 6.0.0 to 6.2.3, 7.0.0 to 7.1.9, and 8.0.0 to 8.0.6 is vulnerable to a HTTP/2 slow read attack.	2020-04-27	5	CVE-2020-9481 CONFIRM DEBIAN
apache -- log4j	Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.	2020-04-27	4.3	CVE-2020-9488 CONFIRM MLIST MLIST MLIST CONFIRM
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to Host header injection by accepting arbitrary host	2020-04-30	5	CVE-2019-12425 CONFIRM
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	2020-04-24	4.3	CVE-2020-12130 MISC
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	2020-04-24	4.3	CVE-2020-12129 MISC
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	2020-04-24	4.3	CVE-2020-12131 MISC
avira -- antivirus	Avira Antivirus before 5.0.2003.1821 on Windows allows privilege escalation or a denial of service via abuse of a symlink.	2020-04-26	4.6	CVE-2020-12254 MISC
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount underflow.	2020-04-24	4.6	CVE-2019-15791 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shiftfs_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shiftfs_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	2020-04-24	4.6	CVE-2019-15792 MISC MISC MISC
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	2020-04-24	4.6	CVE-2019-15793 MISC MISC MISC
cybozo -- garoon	Improper authorization vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote authenticated attackers to alter the application's data via the applications 'E-mail' and 'Messages'.	2020-04-28	4	CVE-2020-5566 MISC MISC
cybozo -- garoon	Improper input validation vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows a remote authenticated attacker to alter the application's data via the applications 'Workflow' and 'MultiReport'.	2020-04-28	4	CVE-2020-5565 MISC MISC
cybozo -- garoon	Server-side request forgery (SSRF) vulnerability in Cybozu Garoon 4.6.0 to 4.6.3 allows a remote attacker with an administrative privilege to issue arbitrary HTTP requests to other web servers via V-CUBE Meeting function.	2020-04-28	4	CVE-2020-5562 MISC MISC
cybozu -- garoon	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in Application Menu.	2020-04-28	5	CVE-2020-5567 MISC MISC
cybozu -- garoon	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in the affected product via the API.	2020-04-28	5	CVE-2020-5563 MISC MISC
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to inject arbitrary web script or HTML via the application 'E-mail'.	2020-04-28	4.3	CVE-2020-5564 MISC MISC
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.6.0 to 5.0.0 allows remote attackers to inject arbitrary web script or HTML via the applications 'Messages' and 'Bulletin Board'.	2020-04-28	4.3	CVE-2020-5568 MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the ./etc/ path.	2020-04-24	5	CVE-2020-12128 MISC
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	2020-04-24	4.8	CVE-2020-5870 MISC
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	2020-04-24	6.4	CVE-2020-5869 MISC
gnu -- mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	2020-04-24	4.3	CVE-2020-12137 MISC MLIST MLIST DEBIAN MISC MISC
grafana -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	2020-04-24	4.3	CVE-2020-12245 MISC MISC MISC
grafana -- grafana	Grafana version < 6.7.3 is vulnerable for annotation popup XSS.	2020-04-27	4.3	CVE-2020-12052 CONFIRM
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 2 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1806.	2020-04-27	5.8	CVE-2020-1805 CONFIRM
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 1 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1805 and CVE-2020-1806.	2020-04-27	5.8	CVE-2020-1804 CONFIRM
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure	2020-04-27	5.8	CVE-2020-1806 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	or service abnormal. This is 3 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1805.			
huawei -- lion-al00c_devices	Huawei smartphone Lion-AL00C with versions earlier than 10.0.0.205(C00E202R7P2) have a denial of service vulnerability. An attacker crafted specially file to the affected device. Due to insufficient input validation of the value when executing the file, successful exploit may cause device abnormal.	2020-04-27	4.3	CVE-2020-1880 CONFIRM
huawei -- pcmanager	Huawei PCManager product with versions earlier than 10.0.5.53 have a local privilege escalation vulnerability. An authenticated, local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2020-04-27	4.6	CVE-2020-1845 CONFIRM
ibm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 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: 173310.	2020-04-24	6.8	CVE-2019-4750 XF CONFIRM
ibm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the implementation of the offering. IBM X-Force ID: 173311.	2020-04-24	5	CVE-2019-4751 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 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: 172519.	2020-04-27	4	CVE-2019-4729 XF CONFIRM CONFIRM
ibm -- mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	2020-04-24	4	CVE-2020-4267 XF CONFIRM
ibm -- websphere_application_server_and_liberty	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM X-Force ID: 177841.	2020-04-28	4	CVE-2020-4329 XF CONFIRM
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows session fixation via an alphanumeric value in a session cookie.	2020-04-29	6.4	CVE-2020-12467 MISC
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows CSV injection via a phrase value within a language. This is related to phrases/add/ and languages/download/.	2020-04-29	6.8	CVE-2020-12468 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mailbeez -- mailbeez	Cross-site scripting (XSS) vulnerability in mailhive/cloudbeez/cloudloader.php and mailhive/cloudbeez/cloudloader_core.php in the MailBeez plugin for ZenCart before 3.9.22 allows remote attackers to inject arbitrary web script or HTML via the cloudloader_mode parameter.	2020-04-30	4.3	CVE-2020-6579 MISC
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI. *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	4.3	CVE-2020-6827 MISC MISC
mozilla -- firefox_esr	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution. *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	6.4	CVE-2020-6828 MISC MISC
mozilla -- multiple_products	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	5	CVE-2020-6821 MISC UBUNTU MISC MISC MISC
mozilla -- multiple_products	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	6.8	CVE-2020-6820 MISC UBUNTU MISC MISC
mozilla -- multiple_products	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	6.8	CVE-2020-6819 MISC UBUNTU MISC MISC
mozilla -- multiple_products	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code>. It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	6.8	CVE-2020-6822 MISC UBUNTU MISC MISC MISC
netgate -- pfsense	An XSS vulnerability resides in the hostname field of the diag_ping.php page in pfsense before 2.4.5 version. After passing	2020-04-29	4.3	CVE-2020-10797 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inputs to the command and executing this command, the $result variable is not sanitized before it is printed.			MISC MISC
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	2020-04-24	5.2	CVE-2017-18698 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	5.8	CVE-2018-21213 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21194 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21193 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200 before 1.0.3.84, and EX7000 before 1.0.0.60.	2020-04-24	4.3	CVE-2017-18715 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	5.2	CVE-2018-21228 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18723 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	2020-04-24	4.8	CVE-2018-21230 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	2020-04-24	4.8	CVE-2018-21231 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500 before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	2020-04-24	4.3	CVE-2017-18700 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-24	6.8	CVE-2017-18703 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18727 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21189 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21191 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18722 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21187 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18729 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18728 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18726 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24. R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18725 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18724 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21192 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	5.2	CVE-2018-21227 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	5.2	CVE-2018-21173 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18721 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.	2020-04-28	5.8	CVE-2018-21216 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18718 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18717 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18716 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18730 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	2020-04-24	5.8	CVE-2017-18705 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.28, EX2700 before 1.0.1.32, EX6200v2 before 1.0.1.56, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before	2020-04-28	6.5	CVE-2018-21181 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.0.3.6, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.52, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	6.5	CVE-2018-21177 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	2020-04-24	5.8	CVE-2017-18731 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX2700 before 1.0.1.28, R7800 before 1.0.2.40, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-27	5.8	CVE-2018-21170 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	CVE-2018-21190 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.98.	2020-04-27	5.2	CVE-2018-21171 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	5.2	CVE-2018-21180 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	5.2	CVE-2018-21179 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	5.2	CVE-2018-21178 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	5.2	CVE-2018-21172 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	5.2	CVE-2018-21182 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, and R9000 before 1.0.2.52.	2020-04-28	5.8	CVE-2018-21221 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.	2020-04-28	5.8	CVE-2018-21217 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18720 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.1.00.26, R6080 before 1.1.00.26; R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	CVE-2017-18719 CONFIRM
netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	2020-04-24	4.8	CVE-2017-18702 CONFIRM
netgear -- r6700_and_r6900_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	2020-04-24	4.3	CVE-2017-18701 CONFIRM
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04-24	5.2	CVE-2017-18699 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.3.6.	2020-04-28	5.2	CVE-2018-21200 CONFIRM
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04-24	5.2	CVE-2017-18697 CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	5.2	CVE-2018-21099 CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	5.2	CVE-2018-21098 CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.46 are affected by incorrect configuration of security settings.	2020-04-27	5.8	CVE-2018-21158 CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	5.2	CVE-2018-21100 CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020-04-24	4.6	CVE-2017-18709 CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	5.2	CVE-2017-18707 CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020-04-24	6.8	CVE-2017-18708 CONFIRM
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability in the comment tags.	2020-04-29	6	CVE-2020-8775 CONFIRM MISC
pegasystems -- pega_platform	The Richtext Editor in Pega Platform before 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability.	2020-04-29	6	CVE-2020-8773 CONFIRM
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Reflected Cross-Site Scripting vulnerability in the "ActionStringID" function.	2020-04-29	6.8	CVE-2020-8774 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	2020-04-24	4	CVE-2020-1741 CONFIRM
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager 2.x before 2.14.17 and 3.x before 3.22.1. Admin users can retrieve the LDAP server system username/password (as configured in nxrm) in cleartext.	2020-04-27	4	CVE-2020-11415 CONFIRM
teampass -- teampass	TeamPass 2.1.27.36 allows an unauthenticated attacker to retrieve files from the TeamPass web root. This may include backups or LDAP debug files.	2020-04-29	5	CVE-2020-12478 MISC
teampass -- teampass	TeamPass 2.1.27.36 allows any authenticated TeamPass user to trigger a PHP file include vulnerability via a crafted HTTP request with sources/users.queries.php newValue directory traversal.	2020-04-29	6.5	CVE-2020-12479 MISC
whoopsie_project -- whoopsie	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	2020-04-24	4.3	CVE-2020-12135 MISC MISC MISC
windriver -- vxworks	The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.	2020-04-27	5	CVE-2020-10664 CONFIRM
wordpress -- wordpress	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information disclosure vulnerability in every ajax search request via the sql field to includes/class-aws-search.php.	2020-04-24	5	CVE-2020-12070 MISC MISC MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bluezone_global -- bluezone	React Native Bluetooth Scan in Bluezone 1.0.0 uses six-character alphanumeric IDs, which might make it easier for remote attackers to interfere with COVID-19 contact tracing by using many IDs.	2020-04-27	3.3	CVE-2020-12270 MISC MISC MISC MISC MISC MISC
croogo -- croogo	Croogo before 3.0.7 allows XSS via the title to admin/menus/menus or admin/taxonomy/vocabularies.	2020-04-26	3.5	CVE-2019-20789 MISC MISC
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.188(C00E74R3P8) have an improper authorization vulnerability. The software does not properly restrict certain user's modification of certain configuration file, successful exploit could allow the attacker to bypass app lock after a series of operation in ADB mode.	2020-04-27	3.6	CVE-2020-1807 CONFIRM
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly senstiive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160514.	2020-04-29	2.1	CVE-2019-4286 XF CONFIRM
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly senstiive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160631.	2020-04-29	2.1	CVE-2019-4288 XF CONFIRM
mozilla -- firefox	Initially, a user opens a Private Browsing Window and generates a password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than independent. This vulnerability affects Firefox < 75.	2020-04-24	1.9	CVE-2020-6824 MISC MISC
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26,	2020-04-24	3.3	CVE-2017-18704 CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	3.3	CVE-2017-18712 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	3.3	CVE-2017-18713 CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	3.3	CVE-2018-21229 CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	3.3	CVE-2017-18710 CONFIRM
netgear -- srr60_and_srs60_devices	Certain NETGEAR devices are affected by stored XSS. This affects SRR60 before 2.2.1.210 and SRS60 before 2.2.1.210.	2020-04-27	2.3	CVE-2018-21095 CONFIRM
netgear -- wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	2020-04-24	3.3	CVE-2017-18714 CONFIRM
ni_consulting -- sales_force_assistant	Cross-site scripting vulnerability in Sales Force Assistant version 11.2.48 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-04-28	3.5	CVE-2020-5570 JVN MISC MISC