SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 April 2020

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-12079	Beaker before 0.8.9 allows a sandbox escape, enabling system access and code execution. This occurs because Electron context isolation is not used, and therefore an attacker can conduct a prototype-pollution attack against the Electron internal messaging API.	10.0	More Details
CVE-2020-11011	In Phproject before version 1.7.8, there's a vulnerability which allows users with access to file uploads to execute arbitrary code. This is patched in version 1.7.8.	9.9	More Details
CVE-2020-7055	An issue was discovered in Elementor 2.7.4. Arbitrary file upload is possible in the Elementor Import Templates function, allowing an attacker to execute code via a crafted ZIP archive.	9.9	More Details
CVE-2020-11690	In JetBrains IntelliJ IDEA before 2020.1, the license server could be resolved to an untrusted host in some cases.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12278	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. path.c mishandles equivalent filenames that exist because of NTFS Alternate Data Streams. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1352.	9.8	More Details
CVE-2020-12265	The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.	9.8	More Details
CVE-2020-12267	setMarkdown in Qt before 5.14.2 has a use-after-free related to QTextMarkdownImporter::insertBlock.	9.8	More Details
CVE-2020-12268	jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow.	9.8	More Details
CVE-2020-12271	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)	9.8	More Details
CVE-2020-12274	In TestLink 1.9.20, the lib/cfields/cfieldsExport.php goback_url parameter causes a security risk because it depends on client input and is not constrained to lib/cfields/cfieldsView.php at the web site associated with the session.	9.8	More Details
CVE-2019-20790	OpenDMARC through 1.3.2 and 1.4.x, when used with pypolicyd-spf 2.0.2, allows attacks that bypass SPF and DMARC authentication in situations where the HELO field is inconsistent with the MAIL FROM field.	9.8	More Details
CVE-2019-18823	HTCondor up to and including stable series 8.8.6 and development series 8.9.4 has Incorrect Access Control. It is possible to use a different authentication method to submit a job than the administrator has specified. If the administrator has configured the READ or WRITE methods to include CLAIMTOBE, then it is possible to impersonate another user to the condor_schedd. (For example to submit or remove jobs)	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11817	In Rukovoditel V2.5.2, attackers can upload an arbitrary file to the server just changing the the content-type value. As a result of that, an attacker can execute a command on the server. This specific attack only occurs with the Maintenance Mode setting.	9.8	More Details
CVE-2020-12133	The Apros Evolution, ConsciusMap, and Furukawa provisioning systems through 2.8.1 allow remote code execution because of javax.faces.ViewState Java deserialization.	9.8	More Details
CVE-2018-21097	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WAC120 before 2.1.7, WN604 before 3.3.10, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, and WND930 before 2.1.5.	9.8	More Details
CVE-2020-9068	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.	9.8	More Details
CVE-2020-1952	An issue was found in Apache IoTDB .9.0 to 0.9.1 and 0.8.0 to 0.8.2. When starting IoTDB, the JMX port 31999 is exposed with no certification.Then, clients could execute code remotely.	9.8	More Details
CVE-2020-12279	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. checkout.c mishandles equivalent filenames that exist because of NTFS short names. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1353.	9.8	More Details
CVE-2020-6826	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.	9.8	More Details
CVE-2020-9294	An improper authentication vulnerability in FortiMail 5.4.10, 6.0.7, 6.2.2 and earlier and FortiVoiceEntreprise 6.0.0 and 6.0.1 may allow a remote unauthenticated attacker to access the system as a legitimate user by requesting a password change via the user interface.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21153	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.62, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	9.8	More Details
CVE-2020-7609	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.	9.8	More Details
CVE-2020-7640	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.	9.8	More Details
CVE-2020-12284	cbs_jpeg_split_fragment in libavcodec/cbs_jpeg.c in FFmpeg 4.1 and 4.2.2 has a heap-based buffer overflow during JPEG_MARKER_SOS handling because of a missing length check.	9.8	More Details
CVE-2017-18857	The NETGEAR Insight application before 2.42 for Android and iOS is affected by password mismanagement.	9.8	More Details
CVE-2017-18858	Certain NETGEAR devices are affected by command execution. This affects M4200-10MG-POE+ 12.0.2.11 and earlier, M4300-28G 12.0.2.11 and earlier, M4300-52G 12.0.2.11 and earlier, M4300-28G-POE+ 12.0.2.11 and earlier, M4300-52G-POE+ 12.0.2.11 and earlier, M4300-8X8F 12.0.2.11 and earlier, M4300-12X12F 12.0.2.11 and earlier, M4300-24X24F 12.0.2.11 and earlier, M4300-24X 12.0.2.11 and earlier, and M4300-48X 12.0.2.11 and earlier.	9.8	More Details
CVE-2019-20791	OpenThread before 2019-12-13 has a stack-based buffer overflow in MeshCoP::Commissioner::GeneratePskc.	9.8	More Details
CVE-2020-12429	Online Course Registration 2.0 has multiple SQL injections that would can lead to a complete database compromise and authentication bypass in the login pages: admin/change-password.php, admin/check_availability.php, admin/index.php, change-password.php, check_availability.php, includes/header.php, index.php, and pincode-verification.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7133	A unauthorized remote access vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	9.8	More Details
CVE-2020-6823	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.	9.8	More Details
CVE-2020-6825	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 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.	9.8	More Details
CVE-2018-21132	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	9.8	More Details
CVE-2019-20787	Teeworlds before 0.7.4 has an integer overflow when computing a tilemap size.	9.8	More Details
CVE-2020-7487	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers.	9.8	More Details
CVE-2020-7489	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability exists on EcoStruxure Machine Expert – Basic or SoMachine Basic programming software (versions in security notification). The result of this vulnerability, DLL substitution, could allow the transference of malicious code to the controller.	9.8	More Details
CVE-2020-10914	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the PerformHandshake method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-10400.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10915	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HandshakeResult method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-10401.	9.8	More Details
CVE-2019-8359	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. An out of bounds write is present in the data section during 6LoWPAN fragment re-assembly in the face of forged fragment offsets in os/net/ipv6/sicslowpan.c.	9.8	More Details
CVE-2020-11939	In nDPI through 3.2 Stable, the SSH protocol dissector has multiple KEXINIT integer overflows that result in a controlled remote heap overflow in concat_hash_string in ssh.c. Due to the granular nature of the overflow primitive and the ability to control both the contents and layout of the nDPI library's heap memory through remote input, this vulnerability may be abused to achieve full Remote Code Execution against any network inspection stack that is linked against nDPI and uses it to perform network traffic analysis.	9.8	More Details
CVE-2020-11945	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).	9.8	More Details
CVE-2020-4415	IBM Spectrum Protect 7.1 and 8.1 server is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker to execute arbitrary code on the system with the privileges of an administrator or user associated with the Spectrum Protect server or cause the Spectrum Protect server to crash. IBM X-Force ID: 179990.	9.8	More Details
CVE-2019-20788	libvncclient/cursor.c in LibVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.	9.8	More Details
CVE-2020-12442	Ivanti Avalanche 6.3 allows a SQL injection that is vaguely associated with the Apache HTTP Server, aka Bug 683250.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21133	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	9.8	More Details
CVE-2018-21134	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6700 before 1.0.1.48, R7900 before 1.0.2.16, R6900 before 1.0.1.48, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R7000 before 1.0.9.34, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R7900P before 1.4.1.24, R8500 before 1.0.2.122, R8300 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, EX3700 before 1.0.0.72, EX3800 before 1.0.0.72, EX6000 before 1.0.0.32, EX6100 before 1.0.2.24, EX6120 before 1.0.0.42, EX6130 before 1.0.0.24, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, D7000v2 before 1.0.0.51, D6220 before 1.0.0.46, D6400 before 1.0.0.82, and D8500 before 1.0.3.42.	9.8	More Details
CVE-2018-21137	Certain NETGEAR devices are affected by a hardcoded password. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	9.8	More Details
CVE-2018-21161	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.46, and R9000 before 1.0.3.16.	9.8	More Details
CVE-2018-21162	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6400 before 1.0.0.78, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.8, R6300v2 before 1.0.4.6, R6400 before 1.0.1.12, R6700 before 1.0.1.16, R7000 before 1.0.7.10, R7100LG before 1.0.0.42, R7300DST before 1.0.0.44, R7900 before 1.0.1.12, R8000 before 1.0.3.36, R8300 before 1.0.2.74, R8500 before 1.0.2.74, WNDR3400v3 before 1.0.1.14, and WNR3500Lv2 before 1.2.0.48.	9.8	More Details
CVE-2020-12134	Nanometrics Centaur through 4.3.23 and TitanSMA through 4.2.20 mishandle access control for the syslog log.	9.8	More Details
CVE-2020-5868	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.	9.8	More Details
CVE-2020-11796	In JetBrains Space through 2020-04-22, the password authentication implementation was insecure.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11012	MinIO versions before RELEASE.2020-04-23T00-58-49Z have an authentication bypass issue in the MinIO admin API. Given an admin access key, it is possible to perform admin API operations i.e. creating new service accounts for existing access keys - without knowing the admin secret key. This has been fixed and released in version RELEASE.2020-04-23T00-58-49Z.	9.3	More Details
CVE-2020-5869	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.	9.1	More Details
CVE-2019-19106	Improper implementation of Access Control in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows an unauthorized user to access data marked as restricted, such as viewing or editing user profiles and application settings.	9.1	More Details
CVE-2019-19104	The web server in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows access to different endpoints of the application without authenticating by accessing a specific uniform resource locator (URL) , violating the access-control (ACL) rules. This issue allows obtaining sensitive information that may aid in further attacks and privilege escalation.	9.1	More Details
CVE-2018-21131	Certain NETGEAR devices are affected by unauthenticated firmware downgrade. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	9.1	More Details
CVE-2020-7131	This document describes a security vulnerability in Blade Maintenance Entity, Integrated Maintenance Entity and Maintenance Entity products. All J/H-series NonStop systems have a security vulnerability associated with an open UDP port 17185 on the Maintenance LAN which could result in information disclosure, denial-of-service attacks or local memory corruption against the affected system and a complete control of the system may also be possible. This vulnerability exists only if one gains access to the Maintenance LAN to which Blade Maintenance Entity, Integrated Maintenance Entity or Maintenance Entity product is connected. **Workaround:** Block the UDP port 17185(In the Maintenance LAN Network Switch/Firewall). Fix: Install following SPRs, which are already available: * T1805A01^AAI (Integrated Maintenance Entity) * T4805A01^AAZ (Blade Maintenance Entity). These SPRs are also usable with the following RVUs: * J06.19.00 ? J06.23.01. No fix planned for the following RVUs: J06.04.00 ? J06.18.01. No fix planned for H-Series NonStop systems. No fix planned for the product T2805 (Maintenance Entity).	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2018-21210	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, EX2700 before 1.0.1.28, 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, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, 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.	8.8	More Details
CVE-2017-18739	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6220 before V1.1.0.50, R7800 before V1.0.2.36, WNDR3400v3 before 1.0.1.14, and WNDR3700v5 before V1.1.0.48.	8.8	More Details
CVE-2020-12138	AMD ATI atillk64.sys 5.11.9.0 allows low-privileged users to interact directly with physical memory by calling one of several driver routines that map physical memory into the virtual address space of the calling process. This could enable low-privileged users to achieve NT AUTHORITY\SYSTEM privileges via a DeviceIoControl call associated with MmMapIoSpace, IoAllocateMdl, MmBuildMdlForNonPagedPool, or MmMapLockedPages.	8.8	More Details
CVE-2017-18742	Certain NETGEAR devices are affected by CSRF. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6250 before 1.0.4.12, R6300v2 before 1.0.4.8, R6700 before 1.0.1.16, R6900 before 1.0.1.16, R7300DST before 1.0.0.54, R7900 before 1.0.1.12, R8000 before 1.0.3.32, and R8500 before 1.0.2.74.	8.8	More Details
CVE-2017-18743	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	8.8	More Details
CVE-2017-18744	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21212	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, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, 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, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, 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.	8.8	More Details
CVE-2017-18748	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX6200v2 before 1.0.1.44, R6100 before 1.0.1.12, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, R7800 before 1.0.2.28, R9000 before 1.0.2.30, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	8.8	More Details
CVE-2017-18749	Certain NETGEAR devices are affected by CSRF. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	8.8	More Details
CVE-2017-18750	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.	8.8	More Details
CVE-2017-18751	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	8.8	More Details
CVE-2017-18732	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18733	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R7100LG before 1.0.0.32, R7300DST before 1.0.0.52, R8300 before 1.0.2.94, and R8500 before 1.0.2.100.	8.8	More Details
CVE-2017-18734	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	8.8	More Details
CVE-2017-18735	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, and R6900v2 before 1.2.0.4.	8.8	More Details
CVE-2017-18736	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, and WNDR3700v5 before 1.1.0.48.	8.8	More Details
CVE-2017-18737	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	8.8	More Details
CVE-2018-21213	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21214	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, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	8.8	More Details
CVE-2020-4202	IBM UrbanCode Deploy (UCD) 7.0.3.0 and 7.0.4.0 could allow an authenticated user to impersonate another user if the server is configured to enable Distributed Front End (DFE). IBM X-Force ID: 174955.	8.8	More Details
CVE-2020-12073	The responsive-add-ons plugin before 2.2.7 for WordPress has incorrect access control for wp-admin/admin-ajax.php?action= requests.	8.8	More Details
CVE-2018-21128	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	8.8	More Details
CVE-2018-21130	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	8.8	More Details
CVE-2020-10890	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829.	8.8	More Details
CVE-2020-10892	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830.	8.8	More Details
CVE-2018-21221	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21220	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, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details
CVE-2020-12075	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks capability checks for AJAX actions.	8.8	More Details
CVE-2018-21215	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, EX2700 before 1.0.1.28, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	8.8	More Details
CVE-2020-12076	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks CSRF nonce checks for AJAX actions. One consequence of this is stored XSS.	8.8	More Details
CVE-2020-12077	The mappress-google-maps-for-wordpress plugin before 2.53.9 for WordPress does not correctly implement AJAX functions with nonces (or capability checks), leading to remote code execution.	8.8	More Details
CVE-2018-21219	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, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details
CVE-2018-21218	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, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21217	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.	8.8	More Details
CVE-2018-21216	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.	8.8	More Details
CVE-2017-18738	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX6150v2 before 1.0.1.54, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R6900P before 1.2.0.22, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R6100 before 1.0.1.16, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	8.8	More Details
CVE-2018-21211	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, D7800 before 1.0.1.30, 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, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details
CVE-2018-21222	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, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details
CVE-2018-21208	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	8.8	More Details
CVE-2017-18716	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18717	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.	8.8	More Details
CVE-2017-18718	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.	8.8	More Details
CVE-2017-18719	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.	8.8	More Details
CVE-2017-18720	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.	8.8	More Details
CVE-2017-18721	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.	8.8	More Details
CVE-2017-18722	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.	8.8	More Details
CVE-2017-18723	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.	8.8	More Details
CVE-2017-18724	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.	8.8	More Details
CVE-2017-18725	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18726	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.	8.8	More Details
CVE-2017-18727	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.	8.8	More Details
CVE-2020-6822	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.	8.8	More Details
CVE-2017-18703	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.	8.8	More Details
CVE-2017-18705	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.	8.8	More Details
CVE-2016-11056	Certain NETGEAR devices are affected by anonymous root access. This affects ReadyNAS Surveillance 1.1.1-3-armel and earlier and ReadyNAS Surveillance 1.4.1-3-amd64 and earlier.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18711	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, 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, 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.	8.8	More Details
CVE-2017-18708	Certain NETGEAR devices are affected by CSRF. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	8.8	More Details
CVE-2018-21203	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6100 before 1.0.1.20, 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.	8.8	More Details
CVE-2018-21102	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	8.8	More Details
CVE-2018-21093	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D8500 before 1.0.3.42, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300-2CXNAS before 1.0.3.60, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R7100LG before 1.0.0.46, R7300 before 1.0.0.68, R7900 before 1.0.2.10, R8000 before 1.0.4.18, R8000P before 1.3.0.10, R7900P before 1.3.0.10, R8500 before 1.0.2.122, R8300 before 1.0.2.122, RBW30 before 2.1.2.6, WN2500RPv2 before 1.0.0.54, and WNR3500Lv2 before 1.2.0.56.	8.8	More Details
CVE-2018-21207	Certain NETGEAR devices are affected by a stack-based 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, EX2700 before 1.0.1.28, 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, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, 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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21206	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, EX2700 before 1.0.1.28, 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, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, 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.	8.8	More Details
CVE-2018-21205	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, EX2700 before 1.0.1.28, 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, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, 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.	8.8	More Details
CVE-2018-21204	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects 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.	8.8	More Details
CVE-2018-21138	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	8.8	More Details
CVE-2017-18731	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.	8.8	More Details
CVE-2018-21202	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects 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 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	8.8	More Details
CVE-2018-21160	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12078	An issue was discovered in Open-AudIT 3.3.1. There is shell metacharacter injection via attributes to an open-audit/configuration/ URI. An attacker can exploit this by adding an excluded IP address to the global discovery settings (internally called exclude_ip). This exclude_ip value is passed to the exec function in the discoveries_helper.php file (inside the all_ip_list function) without being filtered, which means that the attacker can provide a payload instead of a valid IP address.	8.8	More Details
CVE-2017-18728	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.	8.8	More Details
CVE-2017-18729	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.	8.8	More Details
CVE-2017-18730	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.	8.8	More Details
CVE-2018-21127	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	8.8	More Details
CVE-2020-12074	The users-customers-import-export-for-wp-woocommerce plugin before 1.3.9 for WordPress allows subscribers to import administrative accounts via CSV.	8.8	More Details
CVE-2019-4750	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.	8.8	More Details
CVE-2017-18755	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.4.8, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000P before 1.0.0.86, R6900P before 1.0.0.56, R7300 before 1.0.0.54, R8300 before 1.0.2.106, R8500 before 1.0.2.106, DGN2200v4 before 1.0.0.86, DGND2200Bv4 before 1.0.0.86, R6050 before 1.0.0.86, JR6150 before 1.0.1.10, R6220 before 1.1.0.50, and WNDR3700v5 before V1.1.0.48.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21224	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, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details
CVE-2018-21126	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	8.8	More Details
CVE-2018-21125	NETGEAR WAC510 devices before 5.0.0.17 are affected by authentication bypass.	8.8	More Details
CVE-2018-21124	NETGEAR WAC510 devices before 5.0.0.17 are affected by privilege escalation.	8.8	More Details
CVE-2017-18772	Certain NETGEAR devices are affected by authentication bypass. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, R8500 before 1.0.2.74, and WNR2000v2 before 1.2.0.8.	8.8	More Details
CVE-2018-21123	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WC7500 before 6.5.3.9, WC7520 before 6.5.3.9, WC7600v1 before 6.5.3.9, and WC7600v2 before 6.5.3.9.	8.8	More Details
CVE-2018-21121	Certain NETGEAR devices are affected by authentication bypass. This affects GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	8.8	More Details
CVE-2018-21158	NETGEAR R7800 devices before 1.0.2.46 are affected by incorrect configuration of security settings.	8.8	More Details
CVE-2018-21118	NETGEAR XR500 devices before 2.3.2.32 are affected by authentication bypass.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18768	Certain NETGEAR devices are affected by CSRF. This affects EX6100 before 1.0.2.16_1.1.130, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.50, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, and WN3000RPv3 before 1.0.2.44.	8.8	More Details
CVE-2017-18775	Certain NETGEAR devices are affected by CSRF. This affects R6100 before 1.0.1.12, R7500 before 1.0.0.108, WNDR3700v4 before 1.0.2.86, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.42.	8.8	More Details
CVE-2017-18764	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6100 before 1.0.1.14, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, R7500 before 1.0.0.110, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	8.8	More Details
CVE-2018-21170	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.	8.8	More Details
CVE-2020-11941	An issue was discovered in Open-AudIT 3.2.2. There is OS Command injection in Discovery.	8.8	More Details
CVE-2017-18762	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D3600 before 1.0.0.68, D6000 before 1.0.0.68, D6100 before 1.0.0.57, R6100 before 1.0.1.16, R6900P before 1.2.0.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18756	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.66, D8500 before 1.0.3.35, DGN2200Bv4 before 1.0.0.94, DGN2200v4 before 1.0.0.94, R6250 before 1.0.4.14, 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 1.0.1.30, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7900 before 1.0.2.4, R8000 before 1.0.4.2, WN2500RPv2 before 1.0.1.50, WNDR3400v3 before 1.0.1.14, and WNDR4000 before 1.0.2.10.	8.8	More Details
CVE-2018-21223	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, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	8.8	More Details
CVE-2018-21226	Certain NETGEAR devices are affected by authentication bypass. This affects JNR1010v2 before 1.1.0.48, JWNR2010v5 before 1.1.0.48, WNR1000v4 before 1.1.0.48, WNR2020 before 1.1.0.48, and WNR2050 before 1.1.0.48.	8.8	More Details
CVE-2017-18782	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JR6150 before 1.0.1.12, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	8.8	More Details
CVE-2017-18781	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, JR6150 before 1.0.1.12, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21113	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.58, D7800 before 1.0.1.42, R6100 before 1.0.1.28, R7500 before 1.0.0.130, R7500v2 before 1.0.3.36, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, and WNDR4500v3 before 1.0.0.56.	8.8	More Details
CVE-2018-21169	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7000 before 2018-03-01, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 2018-03-01, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	8.8	More Details
CVE-2018-21115	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	8.8	More Details
CVE-2018-21116	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	8.8	More Details
CVE-2018-21117	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers via the traceroute handler.	8.8	More Details
CVE-2020-8477	The installations for ABB System 800xA Information Manager versions 5.1, 6.0 to 6.0.3.2 and 6.1 wrongly contain an auxiliary component. An attacker is able to use this for an XSS-like attack to an authenticated local user, which might lead to execution of arbitrary code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1745	A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before and was fixed in 2.0.30.Final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.	8.6	More Details
CVE-2020-11013	Their is an information disclosure vulnerability in Helm from version 3.1.0 and before version 3.2.0. `lookup` is a Helm template function introduced in Helm v3. It is able to lookup resources in the cluster to check for the existence of specific resources and get details about them. This can be used as part of the process to render templates. The documented behavior of `helm template` states that it does not attach to a remote cluster. However, a the recently added `lookup` template function circumvents this restriction and connects to the cluster even during `helm template` and `helm installlupdateldeletelrollback --dry-run`. The user is not notified of this behavior. Running `helm template` should not make calls to a cluster. This is different from `install`, which is presumed to have access to a cluster in order to load resources into Kubernetes. Helm 2 is unaffected by this vulnerability. A malicious chart author could inject a `lookup` into a chart that, when rendered through `helm template`, performs unannounced lookups against the cluster a user's `KUBECONFIG` file points to. This information can then be disclosed via the output of `helm template`. This issue has been fixed in Helm 3.2.0	8.5	More Details
CVE-2017-18776	Certain NETGEAR devices are affected by authentication bypass. This affects D6100 before V1.0.0.55, D7000 before V1.0.1.50, D7800 before V1.0.1.24, JNR1010v2 before 1.1.0.40, JWNR2010v5 before 1.1.0.40, R6100 before 1.0.1.12, R6220 before 1.1.0.50, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.40, WNR2000v5 before 1.0.0.42, WNR2020 before 1.1.0.40, and WNR2050 before 1.1.0.40.	8.4	More Details
CVE-2020-12118	The keygen protocol implementation in Binance tss-lib before 1.2.0 allows attackers to generate crafted h1 and h2 parameters in order to compromise a signing round or obtain sensitive information from other parties.	8.2	More Details
CVE-2020-7644	fun-map through 3.3.1 is vulnerable to Prototype Pollution. The function assocInM could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5867	In versions prior to 3.3.0, the NGINX Controller Agent installer script 'install.sh' uses HTTP instead of HTTPS to check and install packages	8.1	More Details
CVE-2020-10996	An issue was discovered in Percona XtraDB Cluster before 5.7.28-31.41.2. A bundled script inadvertently sets a static transition_key for SST processes in place of the random key expected.	8.1	More Details
CVE-2020-6819	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.	8.1	More Details
CVE-2020-6820	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.	8.1	More Details
CVE-2020-5870	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.	8.1	More Details
CVE-2020-11539	An issue was discovered on Tata Sonata Smart SF Rush 1.12 devices. It has been identified that the smart band has no pairing (mode 0 Bluetooth LE security level) The data being transmitted over the air is not encrypted. Adding to this, the data being sent to the smart band doesn't have any authentication or signature verification. Thus, any attacker can control a parameter of the device.	8.1	More Details
CVE-2018-21099	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	8.0	More Details
CVE-2018-21120	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	8.0	More Details
CVE-2018-21101	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18758	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	8.0	More Details
CVE-2018-21100	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	8.0	More Details
CVE-2017-18861	Certain NETGEAR devices are affected by CSRF. This affects ReadyNAS Surveillance 1.4.3-15-x86 and earlier and ReadyNAS Surveillance 1.1.4-5-ARM and earlier.	8.0	More Details
CVE-2020-10911	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the GetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9944.	7.8	More Details
CVE-2020-10895	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191.	7.8	More Details
CVE-2020-10912	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the SetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9945.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7135	A potential security vulnerability has been identified in the disk drive firmware installers named Supplemental Update / Online ROM Flash Component on HPE servers running Linux. The vulnerable software is included in the HPE Service Pack for ProLiant (SPP) releases 2018.06.0, 2018.09.0, and 2018.11.0. The vulnerable software is the Supplemental Update / Online ROM Flash Component for Linux (x64) software. The installer in this software component could be locally exploited to execute arbitrary code. Drive Models can be found in the Vulnerability Resolution field of the security bulletin. The 2019_03 SPP and Supplemental update / Online ROM Flash Component for Linux (x64) after 2019.03.0 has fixed this issue.	7.8	More Details
CVE-2020-10893	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10189.	7.8	More Details
CVE-2020-10891	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9831.	7.8	More Details
CVE-2017-18779	Certain NETGEAR devices are affected by a buffer overflow. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10889	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828.	7.8	More Details
CVE-2020-8474	Weak Registry permissions in ABB System 800xA Base allow low privileged users to read and modify registry settings related to control system functionality, allowing an authenticated attacker to cause system functions to stop or malfunction.	7.8	More Details
CVE-2020-10897	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10193.	7.8	More Details
CVE-2020-12254	Avira Antivirus before 5.0.2003.1821 on Windows allows privilege escalation or a denial of service via abuse of a symlink.	7.8	More Details
CVE-2019-20002	Formula Injection exists in the export feature in SolarWinds WebHelpDesk 12.7.1 via a value (provided by a low-privileged user in the Subject field of a help request form) that is mishandled in a TicketActions/view?tab=group TSV export by an admin user.	7.8	More Details
CVE-2020-7490	A CWE-426: Untrusted Search Path vulnerability exists in Vijeo Designer Basic (V1.1 HotFix 15 and prior) and Vijeo Designer (V6.9 SP9 and prior), which could cause arbitrary code execution on the system running Vijeo Basic when a malicious DLL library is loaded by the Product.	7.8	More Details
CVE-2017-18787	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050, before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18786	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	7.8	More Details
CVE-2020-10896	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10192.	7.8	More Details
CVE-2017-18777	Certain NETGEAR devices are affected by administrative password disclosure. This affects D6220 before V1.0.0.28, D6400 before V1.0.0.60, D8500 before V1.0.3.29, DGN2200v4 before 1.0.0.82, DGN2200Bv4 before 1.0.0.82, R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	7.8	More Details
CVE-2020-5740	Improper Input Validation in Plex Media Server on Windows allows a local, unauthenticated attacker to execute arbitrary Python code with SYSTEM privileges.	7.8	More Details
CVE-2020-10898	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10195.	7.8	More Details
CVE-2020-12242	Valve Source allows local users to gain privileges by writing to the /tmp/hl2_relaunch file, which is later executed in the context of a different user account.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10899	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132.	7.8	More Details
CVE-2020-10900	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142.	7.8	More Details
CVE-2020-10913	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OCRAndExportToExcel command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9946.	7.8	More Details
CVE-2020-10902	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10462.	7.8	More Details
CVE-2017-18709	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.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10910	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the RotatePage command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9943.	7.8	More Details
CVE-2020-10904	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10464.	7.8	More Details
CVE-2020-10909	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the AddWatermark command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9942.	7.8	More Details
CVE-2020-10906	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10614.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10908	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Export command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9865.	7.8	More Details
CVE-2020-10907	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of widgets in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10650.	7.8	More Details
CVE-2020-12103	In Tiny File Manager 2.4.1 there is a vulnerability in the ajax file backup copy functionality which allows authenticated users to create backup copies of files (with .bak extension) outside the scope in the same directory in which they are stored.	7.7	More Details
CVE-2020-12102	In Tiny File Manager 2.4.1, there is a Path Traversal vulnerability in the ajax recursive directory listing functionality. This allows authenticated users to enumerate directories and files on the filesystem (outside of the application scope).	7.7	More Details
CVE-2020-11004	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.	7.7	More Details
CVE-2020-6828	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12128	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the ./etc/ path.	7.5	More Details
CVE-2020-10663	The JSON gem through 2.2.0 for Ruby, as used in Ruby 2.4 through 2.4.9, 2.5 through 2.5.7, and 2.6 through 2.6.5, has an Unsafe Object Creation Vulnerability. This is quite similar to CVE-2013-0269, but does not rely on poor garbage-collection behavior within Ruby. Specifically, use of JSON parsing methods can lead to creation of a malicious object within the interpreter, with adverse effects that are application-dependent.	7.5	More Details
CVE-2020-12070	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.	7.5	More Details
CVE-2020-10641	An unprotected logging route may allow an attacker to write endless log statements into the database without space limits or authentication. This results in consuming the entire available hard-disk space on the Ignition 8 Gateway (versions prior to 8.0.10), causing a denial-of-service condition.	7.5	More Details
CVE-2020-11691	In JetBrains Hub before 2020.1.12099, content spoofing in the Hub OAuth error message was possible.	7.5	More Details
CVE-2020-11687	In JetBrains TeamCity before 2019.2.2, password values were shown in an unmasked format on several pages.	7.5	More Details
CVE-2020-11688	In JetBrains TeamCity before 2019.2.1, the application state is kept alive after a user ends his session.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21139	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.58, D6200 before 1.1.00.30, D6220 before 1.0.0.46, D6400 before 1.0.0.82, D7000 before 1.0.1.68, D7000v2 before 1.0.0.51, D7800 before 1.0.1.42, D8500 before 1.0.3.42, DC112A before 1.0.0.40, DGN2200Bv4 before 1.0.0.102, DGN2200v4 before 1.0.0.102, JNR1010v2 before 1.1.0.54, JR6150 before 1.0.1.18, JWNR2010v5 before 1.1.0.54, PR2000 before 1.0.0.24, R6020 before 1.0.0.34, R6050 before 1.0.1.18, R6080 before 1.0.0.34, R6100 before 1.0.1.22, R6120 before 1.0.0.42, R6220 before 1.1.0.68, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R6700 before 1.0.1.48, R6700v2 before 1.2.0.24, R6800 before 1.2.0.24, R6900 before 1.0.1.48, R6900P before 1.3.1.44, R6900v2 before 1.2.0.24, R7000 before 1.0.9.34, R7000P before 1.3.1.44, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R7500 before 1.0.0.124, R7500v2 before 1.0.3.38, R7900 before 1.0.2.16, R7900P before 1.4.1.24, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN3000RP before 1.0.0.68, WN3000RPv2 before 1.0.0.68, WNDR3400v3 before 1.0.1.18, WNDR3700v4 before 1.0.2.102, WNDR3700v5 before 1.1.0.54, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, WNR1000v4 before 1.1.0.54, WNR2020 before 1.1.0.54, WNR2050 before 1.1.0.54, and WNR3500Lv2 before 1.2.0.54.	7.5	More Details
CVE-2020-11693	JetBrains YouTrack before 2020.1.659 was vulnerable to DoS that could be caused by attaching a malformed TIFF file to an issue.	7.5	More Details
CVE-2020-11795	In JetBrains Space through 2020-04-22, the session timeout period was configured improperly.	7.5	More Details
CVE-2020-12243	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	7.5	More Details
CVE-2020-12273	In TestLink 1.9.20, a crafted login.php viewer parameter exposes cleartext credentials.	7.5	More Details
CVE-2020-10664	The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6821	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.	7.5	More Details
CVE-2020-11685	In JetBrains GoLand before 2019.3.2, the plugin repository was accessed via HTTP instead of HTTPS.	7.5	More Details
CVE-2018-21168	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7000 before 1.0.1.52, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	7.5	More Details
CVE-2020-12059	An issue was discovered in Ceph through 13.2.9. A POST request with an invalid tagging XML can crash the RGW process by triggering a NULL pointer exception.	7.5	More Details
CVE-2020-12066	CServer::SendMsg in engine/server/server.cpp in Teeworlds 0.7.x before 0.7.5 allows remote attackers to shut down the server.	7.5	More Details
CVE-2020-12112	BigBlueButton before 2.2.5 allows remote attackers to obtain sensitive files via Local File Inclusion.	7.5	More Details
CVE-2020-11505	An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling.	7.5	More Details
CVE-2016-11058	The NETGEAR genie application before 2.4.34 for Android is affected by mishandling of hard-coded API keys and session IDs.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8867	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC Foundation UA .NET Standard 1.04.358.30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of sessions. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to create a denial-of-service condition against the application. Was ZDI-CAN-10295.	7.5	More Details
CVE-2020-5571	SHARP AQUOS series (AQUOS SH-M02 build number 01.00.05 and earlier, AQUOS SH-RM02 build number 01.00.04 and earlier, AQUOS mini SH-M03 build number 01.00.04 and earlier, AQUOS Keitai SH-N01 build number 01.00.01 and earlier, AQUOS L2 (UQ mobile/J:COM) build number 01.00.05 and earlier, AQUOS sense lite SH-M05 build number 03.00.04 and earlier, AQUOS sense (UQ mobile) build number 03.00.03 and earlier, AQUOS compact SH-M06 build number 02.00.02 and earlier, AQUOS sense plus SH-M07 build number 02.00.02 and earlier, AQUOS sense2 SH-M08 build number 02.00.05 and earlier, and AQUOS sense2 (UQ mobile) build number 02.00.06 and earlier) allow an attacker to obtain the sensitive information of the device via malicious applications installed on the device.	7.5	More Details
CVE-2019-9183	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. A buffer overflow is present due to an integer underflow during 6LoWPAN fragment processing in the face of truncated fragments in os/net/ipv6/sicslowpan.c. This results in accesses of unmapped memory, crashing the application. An attacker can cause a denial-of-service via a crafted 6LoWPAN frame.	7.5	More Details
CVE-2020-11940	In nDPI through 3.2 Stable, an out-of-bounds read in concat_hash_string in ssh.c can be exploited by a network-positioned attacker that can send malformed SSH protocol messages on a network segment monitored by nDPI's library.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-11059	Certain NETGEAR devices are affected by password exposure. This affects AC1450 before 2017-01-06, C6300 before 2017-01-06, D500 before 2017-01-06, D1500 before 2017-01-06, D3600 before 2017-01-06, D6000 before 2017-01-06, D6100 before 2017-01-06, D6200 before 2017-01-06, D6200B before 2017-01-06, D6300B before 2017-01-06, D6300 before 2017-01-06, DGN1000v3 before 2017-01-06, DGN2200v1 before 2017-01-06, DGN2200v3 before 2017-01-06, DGN2200V4 before 2017-01-06, DGN2200Bv3 before 2017-01-06, DGN2200Bv4 before 2017-01-06, DGND3700v1 before 2017-01-06, DGND3700v2 before 2017-01-06, DGND3700Bv2 before 2017-01-06, JNR1010v1 before 2017-01-06, JNR1010v2 before 2017-01-06, JNR3300 before 2017-01-06, JR6100 before 2017-01-06, JR6150 before 2017-01-06, JWNR2000v5 before 2017-01-06, R2000 before 2017-01-06, R6050 before 2017-01-06, R6100 before 2017-01-06, R6200 before 2017-01-06, R6200v2 before 2017-01-06, R6220 before 2017-01-06, R6250 before 2017-01-06, R6300 before 2017-01-06, R6300v2 before 2017-01-06, R6700 before 2017-01-06, R7000 before 2017-01-06, R7900 before 2017-01-06, R7500 before 2017-01-06, R8000 before 2017-01-06, WGR614v10 before 2017-01-06, WNR1000v2 before 2017-01-06, WNR1000v3 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2000v3 before 2017-01-06, WNR2000v4 before 2017-01-06, WNR2000v5 before 2017-01-06, WNR2200 before 2017-01-06, WNR2500 before 2017-01-06, WNR3500Lv2 before 2017-01-06, WNDR3400v2 before 2017-01-06, WNDR3400v3 before 2017-01-06, WNDR3700v3 before 2017-01-06, WNDR3700v4 before 2017-01-06, WNDR3700v5 before 2017-01-06, WNDR4300 before 2017-01-06, WNDR4300v2 before 2017-01-06, WNDR4500v1 before 2017-01-06, WNDR4500v2 before 2017-01-06, and WNDR4500v3 before 2017-01-06.	7.5	More Details
CVE-2016-11060	Certain NETGEAR devices are affected by insecure renegotiation. This affects SRX5308 before 2017-02-10, FVS336Gv3 before 2017-02-10, FVS318N before 2017-02-10, and FVS318Gv2 before 2017-02-10.	7.5	More Details
CVE-2019-14941	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.	7.5	More Details
CVE-2019-15234	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12120	The Correos Express addon for PrestaShop 1.6 through 1.7 allows remote attackers to obtain sensitive information, such as a service's owner password that can be used to modify orders via SOAP. Attackers can also retrieve information about orders or buyers.	7.5	More Details
CVE-2017-18859	Certain NETGEAR devices are affected by slowdown/stoppage. This affects C6300 before 2017-05-30, CM400 before 2017-05-30, CM700 before 2017-05-30, and CMD31T before 2017-05-30.	7.5	More Details
CVE-2020-1983	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a denial of service.	7.5	More Details
CVE-2016-11057	Certain NETGEAR devices are affected by mishandling of repeated URL calls. This affects JNR1010v2 before 2017-01-06, WNR614 before 2017-01-06, WNR618 before 2017-01-06, JWNR2000v5 before 2017-01-06, WNR2020 before 2017-01-06, JWNR2010v5 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2020v2 before 2017-01-06, R6220 before 2017-01-06, and WNDR3700v5 before 2017-01-06.	7.5	More Details
CVE-2020-11506	An issue was discovered in GitLab 10.7.0 and later through 12.9.2. A Workhorse bypass could lead to job artifact uploads and file disclosure (Exposure of Sensitive Information) via request smuggling.	7.5	More Details
CVE-2020-12266	An issue was discovered where there are multiple externally accessible pages that do not require any sort of authentication, and store system information for internal usage. The devices automatically query these pages to update dashboards and other statistics, but the pages can be accessed externally without any authentication. All the pages follow the naming convention live_(string).shtml. Among the information disclosed is: interface status logs, IP address of the device, MAC address of the device, model and current firmware version, location, all running processes, all interfaces and their statuses, all current DHCP leases and the associated hostnames, all other wireless networks in range of the router, memory statistics, and components of the configuration of the device such as enabled features. Affected devices: Affected devices are: Wavlink WN530HG4, Wavlink WN575A3, Wavlink WN579G3,Wavlink WN531G3, Wavlink WN533A8, Wavlink WN531A6, Wavlink WN551K1, Wavlink WN535G3, Wavlink WN530H4, Wavlink WN57X93, WN572HG3, Wavlink WN578A2, Wavlink WN579G3, Wavlink WN579X3, and Jetstream AC3000/ERAC3000	7.5	More Details
CVE-2020-5567	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in Application Menu.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-6859	A CWE-798: Use of Hardcoded Credentials vulnerability exists in Modicon Controllers (All versions of the following CPUs and Communication Module product references listed in the Security Notifications), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.	7.5	More Details
CVE-2020-7067	In PHP versions 7.2.x below 7.2.30, 7.3.x below 7.3.17 and 7.4.x below 7.4.5, if PHP is compiled with EBCDIC support (uncommon), urldecode() function can be made to access locations past the allocated memory, due to erroneously using signed numbers as array indexes.	7.5	More Details
CVE-2020-7488	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers.	7.5	More Details
CVE-2020-9481	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.	7.5	More Details
CVE-2020-5864	In versions of NGINX Controller prior to 3.2.0, communication between NGINX Controller and NGINX Plus instances skip TLS verification by default.	7.4	More Details
CVE-2018-21096	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	7.4	More Details
CVE-2018-21094	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	7.3	More Details
CVE-2018-21174	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, 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.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21175	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.	7.2	More Details
CVE-2018-21135	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700 before 1.0.1.48, R7500 before 1.0.0.124, R7800 before 1.0.2.58, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, and WNR2000v5-R2000 before 1.0.0.68.	7.2	More Details
CVE-2018-21156	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.38, D6400 before 1.0.0.74, D7000v2 before 1.0.0.74, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.102, DGN2200Bv4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.20, R6300v2 before 1.0.4.22, R6400 before 1.0.1.32, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R6900P before 1.3.0.18, R7000 before 1.0.9.28, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900 before 1.0.2.10, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, WN2500RPv2 before 1.0.1.52, WNDR3400v3 before 1.0.1.18, and WNR3500Lv2 before 1.2.0.46.	7.2	More Details
CVE-2018-21181	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 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.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21163	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DGN2200Bv4 before 1.0.0.102, DGN2200v4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6300v2 before 1.0.4.22, R6900P before 1.3.0.18, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, WN2500RPv2 before 1.0.1.52, and WNDR3400v3 before 1.0.1.18.	7.2	More Details
CVE-2018-21177	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.	7.2	More Details
CVE-2018-21176	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, 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.	7.2	More Details
CVE-2018-21164	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6220 before 1.1.0.64 and WNDR3700v5 before 1.1.0.54.	7.2	More Details
CVE-2016-11054	NETGEAR DGN2200v4 devices before 2017-01-06 are affected by command execution and an FTP insecure root directory.	7.2	More Details
CVE-2019-15794	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.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18863	Certain NETGEAR devices are affected by command execution via a PHP form. This affects WN604 3.3.3 and earlier, WNAP210v2 3.5.20.0 and earlier, WNAP320 3.5.20.0 and earlier, WNDAP350 3.5.20.0 and earlier, WNDAP360 3.5.20.0 and earlier, WNDAP620 2.0.11 and earlier, WNDAP660 3.5.20.0 and earlier, WND930 2.0.11 and earlier, and WAC120 2.0.7 and earlier.	7.1	More Details
CVE-2020-1804	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.	7.1	More Details
CVE-2019-15791	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.	7.1	More Details
CVE-2019-15792	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.	7.1	More Details
CVE-2020-1805	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.	7.1	More Details
CVE-2020-1806	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 3 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1805.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4311	IBM Tivoli Monitoring 6.3.0 could allow a local attacker to execute arbitrary code on the system. By placing a specially crafted file, an attacker could exploit this vulnerability to load other DLL files located in the same directory and execute arbitrary code on the system. IBM X-Force ID: 177083.	7.0	More Details
CVE-2020-10712	A flaw was found in OpenShift Container Platform version 4.1 and later. Sensitive information was found to be logged by the image registry operator allowing an attacker able to gain access to those logs, to read and write to the storage backing the internal image registry. The highest threat from this vulnerability is to data integrity.	7.0	More Details
CVE-2020-1762	An insufficient JWT validation vulnerability was found in Kiali versions 0.4.0 to 1.15.0 and was fixed in Kiali version 1.15.1, wherein a remote attacker could abuse this flaw by stealing a valid JWT cookie and using that to spoof a user session, possibly gaining privileges to view and alter the Istio configuration.	7.0	More Details
CVE-2018-21179	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.	6.8	More Details
CVE-2018-21152	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	6.8	More Details
CVE-2018-21191	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.	6.8	More Details
CVE-2018-21180	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.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21171	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.	6.8	More Details
CVE-2018-21157	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R7000 before 1.0.9.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.38, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	6.8	More Details
CVE-2018-21183	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.	6.8	More Details
CVE-2018-21184	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 1.0.1.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, and R9000 before 1.0.3.6.	6.8	More Details
CVE-2018-21154	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, and R7800 before 1.0.2.42.	6.8	More Details
CVE-2018-21185	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, 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.	6.8	More Details
CVE-2018-21190	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.	6.8	More Details
CVE-2018-21192	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.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21189	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.	6.8	More Details
CVE-2018-21149	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.0.54, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	6.8	More Details
CVE-2018-21186	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, 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.	6.8	More Details
CVE-2018-21098	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2018-21187	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.	6.8	More Details
CVE-2018-21178	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.	6.8	More Details
CVE-2018-21188	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, 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.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21182	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.	6.8	More Details
CVE-2018-21172	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.	6.8	More Details
CVE-2018-21193	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.	6.8	More Details
CVE-2018-21108	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2017-18759	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8300 before 1.0.2.104 and R8500 before 1.0.2.104.	6.8	More Details
CVE-2017-18761	NETGEAR R8000 devices before 1.0.4.2 are affected by a stack-based buffer overflow by an authenticated user.	6.8	More Details
CVE-2018-21200	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.	6.8	More Details
CVE-2018-21201	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.	6.8	More Details
CVE-2018-21110	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18767	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6400 before 1.0.1.14, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300 before 1.0.0.56, R7800 before 1.0.2.36, R7900 before 1.0.2.10, R8000 before 1.0.3.24, R8300 before 1.0.2.74, and R8500 before 1.0.2.74.	6.8	More Details
CVE-2018-21109	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2018-21107	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2018-21198	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 1.2.0.44, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.62.	6.8	More Details
CVE-2018-21119	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WAC505 before 5.0.5.4 and WAC510 before 5.0.5.4.	6.8	More Details
CVE-2018-21106	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2018-21105	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2018-21104	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2018-21103	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	6.8	More Details
CVE-2017-18754	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, and WNR2000v5 before 1.0.0.58.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21173	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.	6.8	More Details
CVE-2018-21151	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	6.8	More Details
CVE-2018-21199	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, and WNDR4300 before 1.0.2.98.	6.8	More Details
CVE-2018-21197	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, 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.	6.8	More Details
CVE-2017-18697	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.	6.8	More Details
CVE-2018-21228	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.	6.8	More Details
CVE-2018-21227	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.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18770	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R7800 before 1.0.2.36, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	6.8	More Details
CVE-2018-21194	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.	6.8	More Details
CVE-2017-18699	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.	6.8	More Details
CVE-2018-21196	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, and WNR2000v5 before 1.0.0.62.	6.8	More Details
CVE-2017-18698	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.	6.8	More Details
CVE-2018-21225	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6700 before 1.0.1.30, R6700v2 before 1.2.0.16, R6800 before 1.2.0.16, R6900 before 1.0.1.30, R6900P before 1.2.0.22, R6900v2 before 1.2.0.16, R7000 before 1.0.9.12, R7000P before 1.2.0.22, R7500v2 before 1.0.3.20, R7800 before 1.0.2.44, R8300 before 1.0.2.106, R8500 before 1.0.2.106, and R9000 before 1.0.2.52.	6.8	More Details
CVE-2018-21111	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.60, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.66.	6.8	More Details
CVE-2017-18707	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.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21112	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, and R9000 before 1.0.4.12.	6.8	More Details
CVE-2018-21114	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, EX6150v2 before 1.0.1.70, EX6100v2 before 1.0.1.70, EX6200v2 before 1.0.1.64, EX7300 before 1.0.2.136, EX6400 before 1.0.2.136, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.4.12, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	6.8	More Details
CVE-2018-21195	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, 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.	6.8	More Details
CVE-2018-21150	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	6.8	More Details
CVE-2017-18773	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6100 before V1.0.0.55, D7800 before V1.0.1.24, EX6150v2 before 1.0.0.48, R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before V1.0.3.16, R7800 before V1.0.2.36, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.48.	6.7	More Details
CVE-2020-9072	Huawei OSD product with versions earlier than OSD_uwp_9.0.32.0 have a local privilege escalation vulnerability. An authenticated, local attacker can constructs a specific file path to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18788	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before 1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6150v2 before 1.0.1.54, EX6100v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.18, R6900P before 1.3.0.8, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R8000 before 1.0.4.4_1.1.42, R7900P before 1.1.5.14, R8000P before 1.1.5.14, R8300 before 1.0.2.110, R8500 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.14, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	6.7	More Details
CVE-2020-1845	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.	6.7	More Details
CVE-2020-8797	Juplink RX4-1500 v1.0.3 allows remote attackers to gain root access to the Linux subsystem via an unsanitized exec call (aka Command Line Injection), if the undocumented telnetd service is enabled and the attacker can authenticate as admin from the local network.	6.7	More Details
CVE-2017-18741	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.0.1.20, R7000 before 1.0.7.10, R7000P before 1.0.0.58, R6900P before 1.0.0.58, R7100LG before 1.0.0.32, R7900 before 1.0.1.14, R8000 before 1.0.3.22, and R8500 before 1.0.2.94.	6.5	More Details
CVE-2017-18765	Certain NETGEAR devices are affected by denial of service. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R6700 before 1.0.1.20, R6900 before 1.0.1.20, WNR3500Lv2 before 1.2.0.44, and WNR2000v2 before 1.2.0.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4267	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.	6.5	More Details
CVE-2020-11689	In JetBrains TeamCity before 2019.2.1, a user without appropriate permissions was able to import settings from the settings.kts file.	6.5	More Details
CVE-2020-12430	An issue was discovered in qemuDomainGetStatsIOThread in qemu/qemu_driver.c in libvirt 4.10.0 though 6.x before 6.1.0. A memory leak was found in the virDomainListGetStats libvirt API that is responsible for retrieving domain statistics when managing QEMU guests. This flaw allows unprivileged users with a read-only connection to cause a memory leak in the domstats command, resulting in a potential denial of service.	6.5	More Details
CVE-2020-9482	If NiFi Registry 0.1.0 to 0.5.0 uses an authentication mechanism other than PKI, when the user clicks Log Out, NiFi Registry invalidates the authentication token on the client side but not on the server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi Registry.	6.5	More Details
CVE-2017-18704	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, 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.	6.5	More Details
CVE-2017-18714	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	6.5	More Details
CVE-2017-18713	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.	6.5	More Details
CVE-2020-7134	A remote access to sensitive data vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18706	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.20, R7500 before 1.0.0.118, 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.	6.5	More Details
CVE-2017-18862	Certain NETGEAR devices are affected by authentication bypass. This affects JGS516PE before 2017-05-11, JGS524Ev2 before 2017-05-11, JGS524PE before 2017-05-11, GS105Ev2 before 2017-05-11, GS105PE before 2017-05-11, GS108Ev3 before 2017-05-11, GS108PEv3 before 2017-05-11, GS116Ev2 before 2017-05-11, GSS108E before 2017-05-11, GSS116E before 2017-05-11, XS708Ev2 before 2017-05-11, and XS716E before 2017-05-11.	6.5	More Details
CVE-2020-4085	"HCL Connections is vulnerable to possible information leakage and could disclose sensitive information via stack trace to a local user."	6.5	More Details
CVE-2020-12270	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. NOTE: the vendor disputes the relevance of this report because the recipient of an F1 alert will know it was a false alert if contact-history comparison fails (i.e., an F0 is not actually part of the contact history obtained from the device of this recipient, or this recipient is not actually part of the contact history obtained from the device of an F0)	6.5	More Details
CVE-2017-18763	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.42, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	6.5	More Details
CVE-2019-15793	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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18766	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects DST6501 before 1.1.0.6 and WNR2000v2 before 1.2.0.8.	6.5	More Details
CVE-2018-21229	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.	6.5	More Details
CVE-2020-8831	Apport creates a world writable lock file with root ownership in the world writable /var/lock/apport directory. If the apport/ directory does not exist (this is not uncommon as /var/lock is a tmpfs), it will create the directory, otherwise it will simply continue execution using the existing directory. This allows for a symlink attack if an attacker were to create a symlink at /var/lock/apport, changing apport's lock file location. This file could then be used to escalate privileges, for example. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	6.5	More Details
CVE-2020-11649	An issue was discovered in GitLab CE and EE 8.15 through 12.9.2. Members of a group could still have access after the group is deleted.	6.5	More Details
CVE-2017-18746	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	6.5	More Details
CVE-2017-18747	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	6.5	More Details
CVE-2018-21129	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	6.5	More Details
CVE-2017-18712	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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18752	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.94.	6.5	More Details
CVE-2018-21122	Certain NETGEAR devices are affected by denial of service. This affects GS110EMX before 1.0.0.9, GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	6.5	More Details
CVE-2020-11420	UPS Adapter CS141 before 1.90 allows Directory Traversal. An attacker with Admin or Engineer login credentials could exploit the vulnerability by manipulating variables that reference files and by doing this achieve access to files and directories outside the web root folder. An attacker may access arbitrary files and directories stored in the file system, but integrity of the files are not jeopardized as attacker have read access rights only.	6.5	More Details
CVE-2020-10997	Percona XtraBackup before 2.4.20 unintentionally writes the command line to any resulting backup file output. This may include sensitive arguments passed at run time. In addition, when --history is passed at run time, this command line is also written to the PERCONA_SCHEMA.xtrabackup_history table.	6.5	More Details
CVE-2017-18740	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.61, D6000 before 1.0.0.61, D6100 before 1.0.0.55, D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, 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 1.0.0.58.	6.3	More Details
CVE-2019-19105	The backup function in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway saves the current settings and configuration of the application, including credentials of existing user accounts and other configuration's credentials in plaintext.	6.2	More Details
CVE-2019-19107	The Configuration pages in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway for user profiles and services transfer the password in plaintext (although hidden when displayed).	6.2	More Details
CVE-2020-5568	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'.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11014	Electron-Cash-SLP before version 3.6.2 has a vulnerability. All token creators that use the "Mint Tool" feature of the Electron Cash SLP Edition are at risk of sending the minting authority baton to the wrong SLP address. Sending the mint baton to the wrong address will give another party the ability to issue new tokens or permanently destroy future minting capability. This is fixed version 3.6.2.	6.1	More Details
CVE-2020-5564	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'.	6.1	More Details
CVE-2019-20102	The attachment-uploading feature in Atlassian Confluence Server from version 6.14.0 through version 6.14.3, and version 6.15.0 before version 6.15.5 allows remote attackers to achieve stored cross-site- scripting (SXSS) via a malicious attachment with a modified `mimeType` parameter.	6.1	More Details
CVE-2020-11822	In Rukovoditel 2.5.2, there is a stored XSS vulnerability on the application structure --> user access groups page. Thus, an attacker can inject malicious script to steal all users' valuable data.	6.1	More Details
CVE-2020-12129	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	6.1	More Details
CVE-2020-12130	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	6.1	More Details
CVE-2020-12113	BigBlueButton before 2.2.4 allows XSS via closed captions because dangerouslySetInnerHTML in React is used.	6.1	More Details
CVE-2017-18745	Certain NETGEAR devices are affected by stored XSS. This affects R6400 before 1.0.1.14, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	6.1	More Details
CVE-2020-12245	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12054	The Catch Breadcrumb plugin before 1.5.4 for WordPress allows Reflected XSS via the s parameter (a search query). Also affected are 16 themes (if the plugin is enabled) by the same author: Alchemist and Alchemist PRO, Izabel and Izabel PRO, Chique and Chique PRO, Clean Enterprise and Clean Enterprise PRO, Bold Photography PRO, Intuitive PRO, Devotepress PRO, Clean Blocks PRO, Foodoholic PRO, Catch Mag PRO, Catch Wedding PRO, and Higher Education PRO.	6.1	More Details
CVE-2020-12131	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	6.1	More Details
CVE-2020-12132	Fifthplay S.A.M.I before 2019.3_HP2 allows unauthenticated stored XSS via a POST request.	6.1	More Details
CVE-2020-7350	Rapid7 Metasploit Framework versions before 5.0.85 suffers from an instance of CWE-78: OS Command Injection, wherein the libnotify plugin accepts untrusted user-supplied data via a remote computer's hostname or service name. An attacker can create a specially-crafted hostname or service name to be imported by Metasploit from a variety of sources and trigger a command injection on the operator's terminal. Note, only the Metasploit Framework and products that expose the plugin system is susceptible to this issue -- notably, this does not include Rapid7 Metasploit Pro. Also note, this vulnerability cannot be triggered through a normal scan operation -- the attacker would have to supply a file that is processed with the db_import command.	6.1	More Details
CVE-2020-12052	Grafana version < 6.7.3 is vulnerable for annotation popup XSS.	6.1	More Details
CVE-2018-18405	jQuery v2.2.2 allows XSS via a crafted onerror attribute of an IMG element. NOTE: this vulnerability has been reported to be spam entry	6.1	More Details
CVE-2017-18784	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18783	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	6.1	More Details
CVE-2020-12137	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.	6.1	More Details
CVE-2017-18715	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.	6.1	More Details
CVE-2017-18700	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.	6.1	More Details
CVE-2020-6213	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, is vulnerable to reflected Cross-Site Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	6.1	More Details
CVE-2018-21155	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.52, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.4.2, R9000 before 1.0.3.16, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18701	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	6.1	More Details
CVE-2020-11806	In MailStore Outlook Add-in (and Email Archive Outlook Add-in) through 12.1.2, the login process does not validate the validity of the certificate presented by the server.	5.9	More Details
CVE-2020-12105	OpenConnect through 8.08 mishandles negative return values from X509_check_ function calls, which might assist attackers in performing man-in-the-middle attacks.	5.9	More Details
CVE-2020-1741	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.	5.9	More Details
CVE-2020-1760	A flaw was found in the Ceph Object Gateway, where it supports request sent by an anonymous user in Amazon S3. This flaw could lead to potential XSS attacks due to the lack of proper neutralization of untrusted input.	5.8	More Details
CVE-2019-17101	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in firmware versions prior to x.xx of Netatmo Smart Indoor Camera allows an attacker to execute commands on the device. This issue affects: Netatmo Smart Indoor Camera version and prior versions.	5.7	More Details
CVE-2020-8833	Time-of-check Time-of-use Race Condition vulnerability on crash report ownership change in Apport allows for a possible privilege escalation opportunity. If fs.protected_symlinks is disabled, this can be exploited between the os.open and os.chown calls when the Apport cron script clears out crash files of size 0. A symlink with the same name as the deleted file can then be created upon which chown will be called, changing the file owner to root. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	5.6	More Details
CVE-2020-8798	httpd in Juplink RX4-1500 v1.0.3-v1.0.5 allows remote attackers to change or access router settings by connecting to the unauthenticated setup3.htm endpoint from the local network.	5.5	More Details
CVE-2020-5866	In versions of NGINX Controller prior to 3.3.0, the helper.sh script, which is used optionally in NGINX Controller to change settings, uses sensitive items as command-line arguments.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-4668	IBM UrbanCode Deploy (UCD) 7.0.4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171250.	5.5	More Details
CVE-2017-18780	Certain NETGEAR devices are affected by denial of service. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	5.5	More Details
CVE-2017-18778	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D7000 before 1.0.1.52, D7000v2 before 1.0.0.38, D7800 before 1.0.1.24, D8500 before 1.0.3.29, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300v1 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	5.5	More Details
CVE-2019-15876	In FreeBSD 12.1-STABLE before r356089, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r356090, and 11.3-RELEASE before 11.3-RELEASE-p7, driver specific ioctl command handlers in the oce network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to send passthrough commands to the device firmware.	5.5	More Details
CVE-2019-15877	In FreeBSD 12.1-STABLE before r356606 and 12.1-RELEASE before 12.1-RELEASE-p3, driver specific ioctl command handlers in the ixl network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to trigger updates to the device's non-volatile memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18789	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6250 before V1.0.4.8, R6400 before V1.0.1.22, R6400v2 before V1.0.2.32, R7100LG before V1.0.0.32, R7300 before V1.0.0.52, R8300 before V1.0.2.94, R8500 before V1.0.2.100, D6220 before V1.0.0.28, D6400 before V1.0.0.60, and D8500 before V1.0.3.29.	5.5	More Details
CVE-2018-21167	Certain NETGEAR devices are affected by stored XSS. This affects D6100 before 1.0.0.57, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.78, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	5.5	More Details
CVE-2020-12135	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.	5.5	More Details
CVE-2020-1880	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.	5.5	More Details
CVE-2020-9489	A carefully crafted or corrupt file may trigger a System.exit in Tika's OneNote Parser. Crafted or corrupted files can also cause out of memory errors and/or infinite loops in Tika's ICNSParser, MP3Parser, MP4Parser, SAS7BDATParser, OneNoteParser and ImageParser. Apache Tika users should upgrade to 1.24.1 or later. The vulnerabilities in the MP4Parser were partially fixed by upgrading the com.googlecode:isoparser:1.1.22 dependency to org.tallison:isoparser:1.9.41.2. For unrelated security reasons, we upgraded org.apache.cxf to 3.3.6 as part of the 1.24.1 release.	5.5	More Details
CVE-2020-6212	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10093	A cross-site scripting (XSS) vulnerability in Lexmark Pro910 series inkjet and other discontinued products.	5.4	More Details
CVE-2020-12438	An XSS vulnerability exists in the banners.php page of PHP-Fusion 9.03.50. This can be exploited because the only security measure used against XSS is the stripping of SCRIPT tags. A malicious actor can use HTML event handlers to run JavaScript instead of using SCRIPT tags.	5.4	More Details
CVE-2020-11416	JetBrains Space through 2020-04-22 allows stored XSS in Chats.	5.4	More Details
CVE-2020-7642	lazysizes through 5.2.0 allows execution of malicious JavaScript. The following attributes are not sanitized by the video-embed plugin: data-vimeo, data-vimeoparams, data-youtube and data-ytparams which can be abused to inject malicious JavaScript.	5.4	More Details
CVE-2017-18757	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.16, R7500 before 1.0.0.116, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR4300v2 before 1.0.0.48, WNDR4300v1 before 1.0.2.90, and WNDR4500v3 before 1.0.0.48.	5.4	More Details
CVE-2020-7132	A potential security vulnerability has been identified in HPE Onboard Administrator. The vulnerability could be remotely exploited to allow Reflected Cross Site Scripting. HPE has made the following software updates and mitigation information to resolve the vulnerability in HPE Onboard Administrator. * OA 4.95 (Linux and Windows).	5.4	More Details
CVE-2020-5570	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.	5.4	More Details
CVE-2019-18223	ZOOM International Call Recording 6.3.1 suffers from multiple authenticated stored XSS vulnerabilities via the phoneNumber field in the (1) User Edit or (2) User Add form, (3) name field in the Role Add form, (4) name or number field in the Edit Group form, (5) tagKey or tagValue field in the Recording Rules Configuration, or (6) txt_69735:/VemailAddress/value or txt_75767:/VemailFrom/value field in callrec/config.	5.4	More Details
CVE-2020-12261	Open-AudIT 3.3.0 allows an XSS attack after login.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21230	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.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21231	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.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10094	A cross-site scripting (XSS) vulnerability in Lexmark CS31x before LW74.VYL.P273; CS41x before LW74.VY2.P273; CS51x before LW74.VY4.P273; CX310 before LW74.GM2.P273; CX410 & XC2130 before LW74.GM4.P273; CX510 & XC2132 before LW74.GM7.P273; MS310, MS312, MS317 before LW74.PRL.P273; MS410, M1140 before LW74.PRL.P273; MS315, MS415, MS417 before LW74.TL2.P273; MS51x, MS610dn, MS617 before LW74.PR2.P273; M1145, M3150dn before LW74.PR2.P273; MS610de, M3150 before LW74.PR4.P273; MS71x,M5163dn before LW74.DN2.P273; MS810, MS811, MS812, MS817, MS818 before LW74.DN2.P273; MS810de, M5155, M5163 before LW74.DN4.P273; MS812de, M5170 before LW74.DN7.P273; MS91x before LW74.SA.P273; MX31x, XM1135 before LW74.SB2.P273; MX410, MX510 & MX511 before LW74.SB4.P273; XM1140, XM1145 before LW74.SB4.P273; MX610 & MX611 before LW74.SB7.P273; XM3150 before LW74.SB7.P273; MX71x, MX81x before LW74.TU.P273; XM51xx & XM71xx before LW74.TU.P273; MX91x & XM91x before LW74.MG.P273; MX6500e before LW74.JD.P273; C746 before LHS60.CM2.P738; C748, CS748 before LHS60.CM4.P738; C792, CS796 before LHS60.HC.P738; C925 before LHS60.HV.P738; C950 before LHS60.TP.P738; X548 & XS548 before LHS60.VK.P738; X74x & XS748 before LHS60.NY.P738; X792 & XS79x before LHS60.MR.P738; X925 & XS925 before LHS60.HK.P738; X95x & XS95x before LHS60.TQ.P738; 6500e before LHS60.JR.P738;C734 LR.SK.P824 and earlier; C736 LR.SKE.P824 and earlier; E46x LR.LBH.P824 and earlier; T65x LR.JP.P824 and earlier; X46x LR.BS.P824 and earlier; X65x LR.MN.P824 and earlier; X73x LR.FL.P824 and earlier; W850 LP.JB.P823 and earlier; and X86x LP.SP.P823 and earlier.	5.4	More Details
CVE-2017-18702	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	5.4	More Details
CVE-2020-10944	HashiCorp Nomad and Nomad Enterprise up to 0.10.4 contained a cross-site scripting vulnerability such that files from a malicious workload could cause arbitrary JavaScript to execute in the web UI. Fixed in 0.10.5.	5.4	More Details
	There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 1 out of 2 vulnerabilities. Different than CVE-2020-5303. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than		

CVE Number	Description	Base Score	Reference
	9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than		
CVE-2019-5302	9.1.0.350(C10E3R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8), earlier than 9.1.0.350(C636E4R1P13T8) Charlotte-L09C: earlier than 9.1.0.311(C185E4R1P11T8), earlier than 9.1.0.345(C432E8R1P11T8) Charlotte-L29C: earlier than 9.1.0.325(C185E4R1P11T8), earlier than 9.1.0.335(C636E3R1P13T8), earlier than 9.1.0.345(C432E8R1P11T8), earlier than 9.1.0.336(C605E3R1P12T8) Columbia-AL10B: earlier than 9.1.0.333(C00E333R1P1T8) Columbia-L29D: earlier than 9.1.0.350(C461E3R1P11T8), earlier than 9.1.0.350(C185E3R1P12T8), earlier than 9.1.0.350(C10E5R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8) Cornell-AL00A: earlier than 9.1.0.333(C00E333R1P1T8) Cornell-L29A: earlier than 9.1.0.328(C185E1R1P9T8), earlier than 9.1.0.328(C432E1R1P9T8), earlier than 9.1.0.330(C461E1R1P9T8), earlier than 9.1.0.328(C636E2R1P12T8) Emily-L09C: earlier than 9.1.0.336(C605E4R1P12T8), earlier than 9.1.0.311(C185E2R1P12T8), earlier than 9.1.0.345(C432E10R1P12T8) Emily-L29C: earlier than 9.1.0.311(C605E2R1P12T8), earlier than 9.1.0.311(C636E7R1P13T8), earlier than 9.1.0.311(C432E7R1P11T8) Ever-L29B: earlier than 9.1.0.311(C185E3R3P1), earlier than 9.1.0.310(C636E3R2P1), earlier than 9.1.0.310(C432E3R1P12) HUAWEI Mate 20: earlier than 9.1.0.131(C00E131R3P1) HUAWEI Mate 20 Pro: earlier than 9.1.0.310(C185E10R2P1) HUAWEI Mate 20 RS: earlier than 9.1.0.135(C786E133R3P1) HUAWEI Mate 20 X: earlier than 9.1.0.135(C00E133R2P1) HUAWEI P20: earlier than 9.1.0.333(C00E333R1P1T8) HUAWEI P20 Pro: earlier than 9.1.0.333(C00E333R1P1T8) HUAWEI P30: earlier than 9.1.0.193 HUAWEI P30 Pro: earlier than 9.1.0.186(C00E180R2P1) HUAWEI Y9 2019: earlier than 9.1.0.220(C605E3R1P1T8) HUAWEI nova lite 3: earlier than 9.1.0.305(C635E8R2P2) Honor 10 Lite: earlier than 9.1.0.283(C605E8R2P2) Honor 8X: earlier than 9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than 9.1.0.238(C432E1R3P1) Jackman-L22: earlier than 9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than 9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than 9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than 9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than	5.3	More Details

CVE Number	Description	Base Score	Reference
	9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)		
CVE-2020-11821	In Rukovoditel 2.5.2, users' passwords and usernames are stored in a cookie with URL encoding, base64 encoding, and hashing. Thus, an attacker can easily apply brute force on them.	5.3	More Details
CVE-2020-5563	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.	5.3	More Details
CVE-2019-4751	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.	5.3	More Details
	There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 2 out of 2 vulnerabilities. Different than CVE-2020-5302. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than 9.1.0.350(C10E3R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8), earlier than 9.1.0.350(C636E4R1P13T8) Charlotte-L09C: earlier than 9.1.0.311(C185E4R1P11T8), earlier than 9.1.0.345(C432E8R1P11T8) Charlotte-L29C: earlier than 9.1.0.325(C185E4R1P11T8), earlier than 9.1.0.335(C636E3R1P13T8), earlier than 9.1.0.345(C432E8R1P11T8), earlier than 9.1.0.336(C605E3R1P12T8) Columbia-AL10B: earlier than 9.1.0.333(C00E333R1P1T8) Columbia-L29D: earlier than 9.1.0.350(C461E3R1P11T8), earlier than 9.1.0.350(C185E3R1P12T8), earlier than 9.1.0.350(C10E5R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8) Cornell-AL00A: earlier than 9.1.0.333(C00E333R1P1T8) Cornell-L29A: earlier than 9.1.0.328(C185E1R1P9T8), earlier than 9.1.0.328(C432E1R1P9T8), earlier than 9.1.0.330(C461E1R1P9T8), earlier than 9.1.0.328(C636E2R1P12T8) Emily-L09C: earlier than 9.1.0.336(C605E4R1P12T8), earlier than 9.1.0.311(C185E2R1P12T8), earlier than 9.1.0.345(C432E10R1P12T8) Emily-L29C: earlier than 9.1.0.311(C605E2R1P12T8), earlier than 9.1.0.311(C636E7R1P13T8),		

CVE Number	Description	Base Score	Reference
	earlier than 9.1.0.311(C432E7R1P11T8) Ever-L29B: earlier than 9.1.0.311(C185E3R3P1), earlier than 9.1.0.310(C636E3R2P1), earlier than 9.1.0.310(C432E3R1P12) HUAWEI Mate 20: earlier than		
CVE-2019-5303	9.1.0.131(C00E131R3P1) HUAWEI Mate 20 Pro: earlier than 9.1.0.310(C185E10R2P1) HUAWEI Mate 20 RS: earlier than 9.1.0.135(C786E133R3P1) HUAWEI Mate 20 X: earlier than 9.1.0.135(C00E133R2P1) HUAWEI P20: earlier than 9.1.0.333(C00E333R1P1T8) HUAWEI P20 Pro: earlier than 9.1.0.333(C00E333R1P1T8) HUAWEI P30: earlier than 9.1.0.193 HUAWEI P30 Pro: earlier than 9.1.0.186(C00E180R2P1) HUAWEI Y9 2019: earlier than 9.1.0.220(C605E3R1P1T8) HUAWEI nova lite 3: earlier than 9.1.0.305(C635E8R2P2) Honor 10 Lite: earlier than 9.1.0.283(C605E8R2P2) Honor 8X: earlier than 9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than 9.1.0.238(C432E1R3P1) Jackman-L22: earlier than 9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than 9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than 9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than 9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)	5.3	More Details
CVE-2020-1722	A flaw was found in all ipa versions 4.x.x through 4.8.0. When sending a very long password (>= 1,000,000 characters) to the server, the password hashing process could exhaust memory and CPU leading to a denial of service and the website becoming unresponsive. The highest threat from this vulnerability is to system availability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12272	OpenDMARC through 1.3.2 and 1.4.x allows attacks that inject authentication results to provide false information about the domain that originated an e-mail message. This is caused by incorrect parsing and interpretation of SPF/DKIM authentication results, as demonstrated by the example.net(.example.com substring.	5.3	More Details
CVE-2020-7643	paypal-adaptive through 0.4.2 manipulation of JavaScript objects resulting in Prototype Pollution. The PayPal function could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload.	5.3	More Details
CVE-2020-12063	A certain Postfix 2.10.1-7 package could allow an attacker to send an email from an arbitrary-looking sender via a homoglyph attack, as demonstrated by the similarity of \xce\xbf to the 'o' character. This is potentially relevant when the /etc/postfix/sender_login feature is used, because a spoofed outbound message that uses a configured sender address is blocked with a "Sender address rejected: not logged in" error message, but a spoofed outbound message that uses a homoglyph of a configured sender address is not blocked. NOTE: some third parties argue that any missed blocking of spoofed outbound messages - except for exact matches to a sender address in the /etc/postfix/sender_login file - is outside the design goals of Postfix and thus cannot be considered a Postfix vulnerability	5.3	More Details
CVE-2020-7451	In FreeBSD 12.1-STABLE before r358739, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r358740, and 11.3-RELEASE before 11.3-RELEASE-p7, a TCP SYN-ACK or challenge TCP-ACK segment over IPv6 that is transmitted or retransmitted does not properly initialize the Traffic Class field disclosing one byte of kernel memory over the network.	5.3	More Details
CVE-2020-11415	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.	4.9	More Details
CVE-2020-5562	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.	4.9	More Details
CVE-2018-21142	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21165	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	4.9	More Details
CVE-2018-21166	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	4.9	More Details
CVE-2020-11938	In JetBrains TeamCity 2018.2 through 2019.2.1, a project administrator was able to see scrambled password parameters used in a project. The issue was resolved in 2019.2.2.	4.9	More Details
CVE-2018-21159	NETGEAR ReadyNAS devices before 6.9.3 are affected by incorrect configuration of security settings.	4.9	More Details
CVE-2017-18785	Certain NETGEAR devices are affected by XSS. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before 1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6100v2 before 1.0.1.54, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, R6700v2 before 1.2.0.12, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.18, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R7900P before 1.1.5.14, R8000 before 1.0.4.4, R8000P before 1.1.5.14, R8500 before 1.0.2.110, R8300 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.8, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.42, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12071	Anchor 0.12.7 allows admins to cause XSS via crafted post content.	4.8	More Details
CVE-2019-20789	Croogo before 3.0.7 allows XSS via the title to admin/menus/menus or admin/taxonomy/vocabularies.	4.8	More Details
CVE-2018-21209	Certain NETGEAR devices are affected by reflected XSS. This affects JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.10, R6220 before 1.1.0.60, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	4.8	More Details
CVE-2020-5865	In versions prior to 3.3.0, the NGINX Controller is configured to communicate with its Postgres database server over unencrypted channels, making the communicated data vulnerable to interception via man-in-the-middle (MiTM) attacks.	4.8	More Details
CVE-2020-6827	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.	4.7	More Details
CVE-2019-4735	IBM MaaS360 3.96.62 for iOS could allow an attacker with physical access to the device to obtain sensitive information from the agent outside of the container. IBM X-Force ID: 172705.	4.6	More Details
CVE-2020-4353	IBM MaaS360 6.82 could allow a user with pysical access to the device to crash the application which may enable the user to access restricted applications and device settings. IBM X-Force ID: 178505.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18769	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects 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, EX6200v2 before 1.0.1.50, EX7000 before 1.0.0.56, JR6150 before 1.0.1.18, R6050 before 1.0.1.10J, R6100 before 1.0.1.16, R6150 before 1.0.1.10, R6220 before 1.1.0.50, R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.26, R6700v2 before 1.2.0.4, R6800 before 1.0.1.10, R6900 before 1.0.1.26, R6900P before 1.0.0.58, R6900v2 before 1.2.0.4, R7000 before 1.0.9.6, R7000P before 1.0.0.58, R7100LG before 1.0.0.32, R7300 before 1.0.0.54, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.40, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR4300v1 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR3500Lv2 before 1.2.0.44.	4.6	More Details
CVE-2018-21136	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	4.6	More Details
CVE-2020-1774	When user downloads PGP or S/MIME keys/certificates, exported file has same name for private and public keys. Therefore it's possible to mix them and to send private key to the third-party instead of public key. This issue affects ((OTRS)) Community Edition: 5.0.42 and prior versions, 6.0.27 and prior versions. OTRS: 7.0.16 and prior versions.	4.5	More Details
CVE-2018-21095	Certain NETGEAR devices are affected by stored XSS. This affects SRR60 before 2.2.1.210 and SRS60 before 2.2.1.210.	4.3	More Details
CVE-2017-18710	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.	4.3	More Details
CVE-2020-12286	In Octopus Deploy before 2019.12.9 and 2020 before 2020.1.12, the TaskView permission is not scoped to any dimension. For example, a scoped user who is scoped to only one tenant can view server tasks scoped to any other tenant.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-11055	Certain NETGEAR devices are affected by CSRF. This affects CM400 before 2017-01-11, CM600 before 2017-01-11, D1500 before 2017-01-11, D500 before 2017-01-11, DST6501 before 2017-01-11, JNR1010v1 before 2017-01-11, JWNR2000Tv3 before 2017-01-11, JWNR2010v3 before 2017-01-11, PLW1000 before 2017-01-11, PLW1010 before 2017-01-11, WNR500 before 2017-01-11, WNR612v3 before 2017-01-11, N450 before 2017-01-11, and CG3000Dv2 before 2017-01-11.	4.3	More Details
CVE-2020-4329	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.	4.3	More Details
CVE-2020-5565	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'.	4.3	More Details
CVE-2020-5566	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'.	4.3	More Details
CVE-2019-4729	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.	4.3	More Details
CVE-2020-9488	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. Fixed in Apache Log4j 2.12.3 and 2.13.1	3.7	More Details
CVE-2020-11810	An issue was discovered in OpenVPN 2.4.x before 2.4.9. An attacker can inject a data channel v2 (P_DATA_V2) packet using a victim's peer-id. Normally such packets are dropped, but if this packet arrives before the data channel crypto parameters have been initialized, the victim's connection will be dropped. This requires careful timing due to the small time window (usually within a few seconds) between the victim client connection starting and the server PUSH_REPLY response back to the client. This attack will only work if Negotiable Cipher Parameters (NCP) is in use.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1807	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.	3.5	More Details
CVE-2020-11869	An integer overflow was found in QEMU 4.0.1 through 4.2.0 in the way it implemented ATI VGA emulation. This flaw occurs in the ati_2d_blt() routine in hw/display/ati-2d.c while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could abuse this flaw to crash the QEMU process, resulting in a denial of service.	3.3	More Details
CVE-2020-10894	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10190.	3.3	More Details
CVE-2020-10901	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10461.	3.3	More Details
CVE-2020-10905	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of vertices in U3D objects. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10568.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10903	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10463.	3.3	More Details
CVE-2020-6824	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.	2.8	More Details
CVE-2019-15790	Apport reads and writes information on a crashed process to /proc/pid with elevated privileges. Apport then determines which user the crashed process belongs to by reading /proc/pid through get_pid_info() in data/apport. An unprivileged user could exploit this to read information about a privileged running process by exploiting PID recycling. This information could then be used to obtain ASLR offsets for a process with an existing memory corruption vulnerability. The initial fix introduced regressions in the Python Apport library due to a missing argument in Report.add_proc_environ in apport/report.py. It also caused an autopkgtest failure when reading /proc/pid and with Python 2 compatibility by reading /proc maps. The initial and subsequent regression fixes are in 2.20.11-0ubuntu16, 2.20.11-0ubuntu8.6, 2.20.9-0ubuntu7.12, 2.20.1-0ubuntu2.22 and 2.14.1-0ubuntu3.29+esm3.	2.8	More Details
CVE-2020-11692	In JetBrains YouTrack before 2020.1.659, DB export was accessible to read-only administrators.	2.7	More Details
CVE-2020-11686	In JetBrains TeamCity before 2019.1.4, a project administrator was able to retrieve some TeamCity server settings.	2.7	More Details
CVE-2020-10647	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details