SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 29 December 2021

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-2021-23198	mySCADA myPRO: Versions 8.20.0 and prior has a feature where the password can be specified, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	10.0	More Details
CVE-2021-45630	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	10.0	More Details
CVE-2021-22657	mySCADA myPRO: Versions 8.20.0 and prior has a feature where the API password can be specified, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	10.0	More Details
CVE-2021-43981	mySCADA myPRO: Versions 8.20.0 and prior has a feature to send emails, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44453	mySCADA myPRO: Versions 8.20.0 and prior has a vulnerable debug interface which includes a ping utility, which may allow an attacker to inject arbitrary operating system commands.	10.0	More Details
CVE-2021-43984	mySCADA myPRO: Versions 8.20.0 and prior has a feature where the firmware can be updated, which may allow an attacker to inject arbitrary operating system commands through a specific parameter.	10.0	More Details
CVE-2021-21872	An OS command injection vulnerability exists in the Web Manager Diagnostics: Traceroute functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2021-21881	An OS command injection vulnerability exists in the Web Manager Wireless Network Scanner functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2021-21889	A stack-based buffer overflow vulnerability exists in the Web Manager Ping functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2021-21883	An OS command injection vulnerability exists in the Web Manager Diagnostics: Ping functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2021-21892	A stack-based buffer overflow vulnerability exists in the Web Manager FsUnmount functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2021-45683	An issue was discovered in the binjs_io crate through 2021-01-03 for Rust. The Read method may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45686	An issue was discovered in the csv-sniffer crate through 2021-01-05 for Rust. preamble_skipcount may read from uninitialized memory locations.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45687	An issue was discovered in the raw-cpuid crate before 9.1.1 for Rust. If the serialize feature is used (which is not the the default), a Deserialize operation may lack sufficient validation, leading to memory corruption or a panic.	9.8	More Details
CVE-2021-45684	An issue was discovered in the flumedb crate through 2021-01-07 for Rust. read_entry may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45688	An issue was discovered in the ash crate before 0.33.1 for Rust. util::read_spv may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45689	An issue was discovered in the gfx-auxil crate through 2021-01-07 for Rust. gfx_auxil::read_spirv may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45685	An issue was discovered in the columnar crate through 2021-01-07 for Rust. ColumnarReadExt::read_typed_vec may read from uninitialized memory locations.	9.8	More Details
CVE-2021-44029	An issue was discovered in Quest KACE Desktop Authority before 11.2. This vulnerability allows attackers to execute remote code through a deserialization exploitation in the RadAsyncUpload function of ASP.NET AJAX. An attacker can leverage this vulnerability when the encryption keys are known (due to the presence of CVE-2017-11317, CVE-2017-11357, or other means). A default setting for the type whitelisting feature in more current versions of ASP.NET AJAX prevents exploitation.	9.8	More Details
CVE-2021-45682	An issue was discovered in the bronzedb-protocol crate through 2021-01-03 for Rust. ReadKVExt may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45691	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_string may read from uninitialized memory locations.	9.8	More Details
CVE-2020-36514	An issue was discovered in the acc_reader crate through 2020-12-27 for Rust. fill_buf may read from uninitialized memory locations.	9.8	More Details
CVE-2020-36513	An issue was discovered in the acc_reader crate through 2020-12-27 for Rust. read_up_to may read from uninitialized memory locations.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36512	An issue was discovered in the buffoon crate through 2020-12-31 for Rust. InputStream::read_exact may read from uninitialized memory locations.	9.8	More Details
CVE-2018-25026	An issue was discovered in the actix-web crate before 0.7.15 for Rust. It can add the Send marker trait to an object that cannot be sent between threads safely, leading to memory corruption.	9.8	More Details
CVE-2018-25025	An issue was discovered in the actix-web crate before 0.7.15 for Rust. It can unsoundly extend the lifetime of a string, leading to memory corruption.	9.8	More Details
CVE-2018-25024	An issue was discovered in the actix-web crate before 0.7.15 for Rust. It can unsoundly coerce an immutable reference into a mutable reference, leading to memory corruption.	9.8	More Details
CVE-2021-45678	NETGEAR RAX200 devices before 1.0.5.132 are affected by insecure code.	9.8	More Details
CVE-2021-45690	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_binary may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45695	An issue was discovered in the mopa crate through 2021-06-01 for Rust. It incorrectly relies on Trait memory layout, possibly leading to future occurrences of arbitrary code execution or ASLR bypass.	9.8	More Details
CVE-2021-45692	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_extension_others may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45693	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_string_primitive may read from uninitialized memory locations.	9.8	More Details
CVE-2020-7878	An arbitrary file download and execution vulnerability was found in the VideoOffice X2.9 and earlier versions (CVE-2020-7878). This issue is due to missing support for integrity check.	9.8	More Details
CVE-2021-45814	Nettmp NNT 5.1 is affected by a SQL injection vulnerability. An attacker can bypass authentication and access the panel with an administrative account.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37401	An attacker may obtain the user credentials from file servers, backup repositories, or ZLD files saved in SD cards. As a result, the PLC user program may be uploaded, altered, and/or downloaded.	9.8	More Details
CVE-2021-37400	An attacker may obtain the user credentials from the communication between the PLC and the software. As a result, the PLC user program may be uploaded, altered, and/or downloaded.	9.8	More Details
CVE-2019-20082	ASUS RT-N53 3.0.0.4.376.3754 devices have a buffer overflow via a long lan_dns1_x or lan_dns2_x parameter to Advanced_LAN_Content.asp.	9.8	More Details
CVE-2020-21238	An issue in the user login box of CSCMS v4.0 allows attackers to hijack user accounts via brute force attacks.	9.8	More Details
CVE-2020-21237	An issue in the user login box of LJCMS v1.11 allows attackers to hijack user accounts via brute force attacks.	9.8	More Details
CVE-2021-45890	basic/BasicAuthProvider.java in AuthGuard before 0.9.0 allows authentication via an inactive identifier.	9.8	More Details
CVE-2021-4161	The affected products contain vulnerable firmware, which could allow an attacker to sniff the traffic and decrypt login credential details. This could give an attacker admin rights through the HTTP web server.	9.8	More Details
CVE-2021-43857	Gerapy is a distributed crawler management framework. Gerapy prior to version 0.9.8 is vulnerable to remote code execution, and this issue is patched in version 0.9.8.	9.8	More Details
CVE-2021-45232	In Apache APISIX Dashboard before 2.10.1, the Manager API uses two frameworks and introduces framework `droplet` on the basis of framework `gin`, all APIs and authentication middleware are developed based on framework `droplet`, but some API directly use the interface of framework `gin` thus bypassing the authentication.	9.8	More Details
CVE-2021-45709	An issue was discovered in the crypto2 crate through 2021-10-08 for Rust. During Chacha20 encryption and decryption, an unaligned read of a u32 may occur.	9.8	More Details
CVE-2021-45707	An issue was discovered in the nix crate 0.16.0 and later before 0.20.2, 0.21.x before 0.21.2, and 0.22.x before 0.22.2 for Rust. unistd::getgrouplist has an out-of-bounds write if a user is in more than 16 /etc/groups groups.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45706	An issue was discovered in the zeroize_derive crate before 1.1.1 for Rust. Dropped memory is not zeroed out for an enum.	9.8	More Details
CVE-2021-45705	An issue was discovered in the nanorand crate before 0.6.1 for Rust. There can be multiple mutable references to the same object because the TlsWyRand Deref implementation dereferences a raw pointer.	9.8	More Details
CVE-2021-45703	An issue was discovered in the tectonic_xdv crate before 0.1.12 for Rust. XdvParser::<T>::process may read from uninitialized memory locations.	9.8	More Details
CVE-2021-45701	An issue was discovered in the tremor-script crate before 0.11.6 for Rust. A patch operation may result in a use-after-free.	9.8	More Details
CVE-2021-45698	An issue was discovered in the ckb crate before 0.40.0 for Rust. A get_block_template RPC call may fail in situations where it is supposed to select a Nervos CKB blockchain transaction with a higher fee rate than another transaction.	9.8	More Details
CVE-2021-45697	An issue was discovered in the molecule crate before 0.7.2 for Rust. A FixVec partial read has an incorrect result.	9.8	More Details
CVE-2021-45696	An issue was discovered in the sha2 crate 0.9.7 before 0.9.8 for Rust. Hashes of long messages may be incorrect when the AVX2-accelerated backend is used.	9.8	More Details
CVE-2021-44031	An issue was discovered in Quest KACE Desktop Authority before 11.2. /dacomponentui/profiles/profileitems/outlooksettings/Insertimage.aspx contains a vulnerability that could allow pre-authentication remote code execution. An attacker could upload a .ASP file to reside at /images/{GUID}/{filename}.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45617	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX7500 before 1.0.0.72, R6400 before 1.0.1.68, R6900P before 1.3.2.132, R7000 before 1.0.11.116, R7000P before 1.3.2.132, R7900 before 1.0.4.38, R7960P before 1.4.1.66, R8000 before 1.0.4.66, RAX200 before 1.0.3.106, RS400 before 1.5.1.80, XR300 before 1.0.3.68, MK62 before 1.0.6.110, MR60 before 1.0.6.110, R6400v2 before 1.0.4.106, R8000P before 1.4.1.66, RAX20 before 1.0.2.64, RAX45 before 1.0.2.82, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, R6700v3 before 1.0.4.106, R7900P before 1.4.1.66, RAX15 before 1.0.2.64, RAX50 before 1.0.2.82, RAX75 before 1.0.3.106, RBR750 before 3.2.16.22, RBR850 before 3.2.16.22, RBS750 before 3.2.16.22, RBS850 before 3.2.16.22, RBK752 before 3.2.16.22, and RBK852 before 3.2.16.22.	9.8	More Details
CVE-2020-7883	Printchaser v2.2021.804.1 and earlier versions contain a vulnerability, which could allow remote attacker to download and execute remote file by setting the argument, variable in the activeX module. This can be leveraged for code execution.	9.8	More Details
CVE-2021-40418	When parsing a file that is submitted to the DPDecoder service as a job, the R3D SDK will mistakenly skip over the assignment of a property containing an object referring to a UUID that was parsed from a frame within the video container. Upon destruction of the object that owns it, the uninitialized member will be dereferenced and then destroyed using the object's virtual destructor. Due to the object property being uninitialized, this can result in dereferencing an arbitrary pointer for the object's virtual method table, which can result in code execution under the context of the application.	9.8	More Details
CVE-2021-39306	A stack buffer overflow was discovered on Realtek RTL8195AM device before 2.0.10, it exists in the client code when an attacker sends a big size Authentication challenge text in WEP security.	9.8	More Details
CVE-2021-43987	An additional, nondocumented administrative account exists in mySCADA myPRO Versions 8.20.0 and prior that is not exposed through the web interface, which cannot be deleted or changed through the regular web interface.	9.8	More Details
CVE-2021-27007	NetApp Virtual Desktop Service (VDS) when used with an HTML5 gateway is susceptible to a vulnerability which when successfully exploited could allow an unauthenticated attacker to takeover a Remote Desktop Session.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-8703	This issue was addressed with improved entitlements. This issue is fixed in watchOS 6, tvOS 13, macOS Catalina 10.15, iOS 13. An application may be able to gain elevated privileges.	9.8	More Details
CVE-2019-8643	CVE-2019-8643: Arun Sharma of VMWare This issue is fixed in macOS Mojave 10.14. Description: A logic issue was addressed with improved state management..	9.8	More Details
CVE-2021-44526	Zoho ManageEngine ServiceDesk Plus before 12003 allows authentication bypass in certain admin configurations.	9.8	More Details
CVE-2021-44548	An Improper Input Validation vulnerability in DataImportHandler of Apache Solr allows an attacker to provide a Windows UNC path resulting in an SMB network call being made from the Solr host to another host on the network. If the attacker has wider access to the network, this may lead to SMB attacks, which may result in: * The exfiltration of sensitive data such as OS user hashes (NTLM/LM hashes), * In case of misconfigured systems, SMB Relay Attacks which can lead to user impersonation on SMB Shares or, in a worse-case scenario, Remote Code Execution This issue affects all Apache Solr versions prior to 8.11.1. This issue only affects Windows.	9.8	More Details
CVE-2020-20601	An issue in ThinkCMF X2.2.2 and below allows attackers to execute arbitrary code via a crafted packet.	9.8	More Details
CVE-2021-45461	FreePBX, when restapps (aka Rest Phone Apps) 15.0.19.87, 15.0.19.88, 16.0.18.40, or 16.0.18.41 is installed, allows remote attackers to execute arbitrary code, as exploited in the wild in December 2021. The fixed versions are 15.0.20 and 16.0.19.	9.8	More Details
CVE-2021-40417	When parsing a file that is submitted to the DPDecoder service as a job, the service will use the combination of decoding parameters that were submitted with the job along with fields that were parsed for the submitted video by the R3D SDK to calculate the size of a heap buffer. Due to an integer overflow with regards to this calculation, this can result in an undersized heap buffer being allocated. When this heap buffer is written to, a heap-based buffer overflow will occur. This can result in code execution under the context of the application.	9.8	More Details
CVE-2021-40394	An out-of-bounds write vulnerability exists in the RS-274X aperture macro variables handling functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and the forked version of Gerbv (commit 71493260). A specially-crafted gerber file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40393	An out-of-bounds write vulnerability exists in the RS-274X aperture macro variables handling functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and the forked version of Gerbv (commit 71493260). A specially-crafted gerber file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-21952	An authentication bypass vulnerability exists in the CMD_DEVICE_GET_RSA_KEY_REQUEST functionality of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted set of network packets can lead to increased privileges.	9.8	More Details
CVE-2021-21903	A stack-based buffer overflow vulnerability exists in the CMA check_udp_crc function of Garrett Metal Detectors' iC Module CMA Version 5.0. A specially-crafted packet can lead to a stack-based buffer overflow during a call to strcpy. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details
CVE-2021-44659	Adding a new pipeline in GoCD server version 21.3.0 has a functionality that could be abused to do an un-intended action in order to achieve a Server Side Request Forgery (SSRF). NOTE: the vendor's position is that the observed behavior is not a vulnerability, because the product's design allows an admin to configure outbound requests	9.8	More Details
CVE-2021-43631	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via the appointment_no parameter in payment.php.	9.8	More Details
CVE-2021-43629	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via multiple parameters in admin_home.php.	9.8	More Details
CVE-2021-43628	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via the email parameter in hms-staff.php.	9.8	More Details
CVE-2021-43157	Projectsworlds Online Shopping System PHP 1.0 is vulnerable to SQL injection via the id parameter in cart_remove.php.	9.8	More Details
CVE-2021-43155	Projectsworlds Online Book Store PHP v1.0 is vulnerable to SQL injection via the "bookisbn" parameter in cart.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40612	An issue was discovered in Opmantek Open-AudIT after 3.5.0. Without authentication, a vulnerability in code_igniter/application/controllers/util.php allows an attacker perform command execution without echoes.	9.8	More Details
CVE-2021-45459	lib/cmd.js in the node-windows package before 1.0.0-beta.6 for Node.js allows command injection via the PID parameter.	9.8	More Details
CVE-2021-45500	Certain NETGEAR devices are affected by authentication bypass. This affects R7000P before 1.3.3.140 and R8000 before 1.0.4.68.	9.6	More Details
CVE-2021-45638	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.68, D6400 before 1.0.0.102, D7000v2 before 1.0.0.74, D8500 before 1.0.3.60, DC112A before 1.0.0.56, R6300v2 before 1.0.4.50, R6400 before 1.0.1.68, R7000 before 1.0.11.116, R7100LG before 1.0.0.70, RBS40V before 2.6.2.8, RBW30 before 2.6.2.2, RS400 before 1.5.1.80, R7000P before 1.3.2.132, and R6900P before 1.3.2.132.	9.6	More Details
CVE-2021-45652	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	9.6	More Details
CVE-2021-45654	NETGEAR XR1000 devices before 1.0.0.58 are affected by disclosure of sensitive information.	9.6	More Details
CVE-2021-45505	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45506	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-38013	Heap buffer overflow in fingerprint recognition in Google Chrome on ChromeOS prior to 96.0.4664.45 allowed a remote attacker who had compromised a WebUI renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45634	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45635	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45613	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, D7000v2 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, MR80 before 1.1.2.20, MS80 before 1.1.2.20, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX43 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX35v2 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and XR1000 before 1.0.0.58.	9.6	More Details
CVE-2021-45633	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, and RBK852 before 3.2.17.12.	9.6	More Details
CVE-2021-45618	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7800 before 1.0.1.64, EX6200v2 before 1.0.1.86, EX6250 before 1.0.0.134, EX7700 before 1.0.0.216, EX8000 before 1.0.1.232, LBR20 before 2.6.3.50, R7800 before 1.0.2.80, R8900 before 1.0.5.26, R9000 before 1.0.5.26, RAX120 before 1.2.0.16, RBS50Y before 1.0.0.56, WNR2000v5 before 1.0.0.76, XR450 before 2.3.2.114, XR500 before 2.3.2.114, XR700 before 1.0.1.36, EX6150v2 before 1.0.1.98, EX7300 before 1.0.2.158, EX7320 before 1.0.0.134, EX6100v2 before 1.0.1.98, EX6400 before 1.0.2.158, EX7300v2 before 1.0.0.134, EX6410 before 1.0.0.134, RBR10 before 2.6.1.44, RBR20 before 2.6.2.104, RBR40 before 2.6.2.104, RBR50 before 2.7.2.102, EX6420 before 1.0.0.134, RBS10 before 2.6.1.44, RBS20 before 2.6.2.104, RBS40 before 2.6.2.104, RBS50 before 2.7.2.102, EX6400v2 before 1.0.0.134, RBK12 before 2.6.1.44, RBK20 before 2.6.2.104, RBK40 before 2.6.2.104, and RBK50 before 2.7.2.102.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45616	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 3.2.18.2, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, and XR1000 before 1.0.0.58.	9.6	More Details
CVE-2021-45615	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000P before 1.4.2.84, R8300 before 1.0.2.154, R8500 before 1.0.2.154, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45614	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7000v2 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX43 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX35v2 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and XR1000 before 1.0.0.58.	9.6	More Details
CVE-2021-45504	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBR852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45632	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45611	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects DC112A before 1.0.0.52, R6400 before 1.0.1.68, RAX200 before 1.0.3.106, WNDR3400v3 before 1.0.1.38, XR300 before 1.0.3.68, R8500 before 1.0.2.144, RAX75 before 1.0.3.106, R8300 before 1.0.2.144, and RAX80 before 1.0.3.106.	9.6	More Details
CVE-2021-45610	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.66, D6400 before 1.0.0.100, D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, DC112A before 1.0.0.52, DGN2200v4 before 1.0.0.118, EAX80 before 1.0.1.64, R6250 before 1.0.4.48, R7000 before 1.0.11.110, R7100LG before 1.0.0.72, R7900 before 1.0.4.30, R7960P before 1.4.1.64, R8000 before 1.0.4.62, RAX200 before 1.0.3.106, RS400 before 1.5.1.80, XR300 before 1.0.3.68, R6400v2 before 1.0.4.106, R7000P before 1.3.2.132, R8000P before 1.4.1.64, RAX20 before 1.0.2.82, RAX45 before 1.0.2.82, RAX80 before 1.0.3.106, R6700v3 before 1.0.4.106, R6900P before 1.3.2.132, R7900P before 1.4.1.64, RAX15 before 1.0.2.82, RAX50 before 1.0.2.82, and RAX75 before 1.0.3.106.	9.6	More Details
CVE-2021-45609	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D8500 before 1.0.3.58, R6250 before 1.0.4.48, R7000 before 1.0.11.116, R7100LG before 1.0.0.64, R7900 before 1.0.4.38, R8300 before 1.0.2.144, R8500 before 1.0.2.144, XR300 before 1.0.3.68, R7000P before 1.3.2.132, and R6900P before 1.3.2.132.	9.6	More Details
CVE-2021-45527	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.68, D6400 before 1.0.0.102, D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, DC112A before 1.0.0.54, EX7000 before 1.0.1.94, EX7500 before 1.0.0.72, R6250 before 1.0.4.48, R6300v2 before 1.0.4.52, R6400 before 1.0.1.70, R6400v2 before 1.0.4.102, R6700v3 before 1.0.4.102, R7000 before 1.0.11.116, R7100LG before 1.0.0.64, R7850 before 1.0.5.68, R7900 before 1.0.4.30, R7960P before 1.4.1.68, R8000 before 1.0.4.52, RAX200 before 1.0.2.88, RBS40V before 2.6.2.4, RS400 before 1.5.1.80, XR300 before 1.0.3.56, R7000P before 1.3.2.124, R8000P before 1.4.1.68, R8500 before 1.0.2.144, RAX80 before 1.0.3.102, R6900P before 1.3.2.124, R7900P before 1.4.1.68, R8300 before 1.0.2.144, RAX75 before 1.0.3.102, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, and RBK852 before 3.2.17.12.	9.6	More Details
CVE-2021-45520	Certain NETGEAR devices are affected by a hardcoded password. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45514	NETGEAR XR1000 devices before 1.0.0.58 are affected by command injection by an unauthenticated attacker.	9.6	More Details
CVE-2021-45513	NETGEAR XR1000 devices before 1.0.0.58 are affected by command injection by an unauthenticated attacker.	9.6	More Details
CVE-2021-45509	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45508	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, and RBR850 before 3.2.17.12.	9.6	More Details
CVE-2021-45507	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBW30 before 2.6.2.2, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and RBS40V before 2.6.2.8.	9.6	More Details
CVE-2021-45503	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45612	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, EX7500 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7850 before 1.0.5.74, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45619	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects EX6200v2 before 1.0.1.86, EX6250 before 1.0.0.134, EX7700 before 1.0.0.216, EX8000 before 1.0.1.232, LBR1020 before 2.6.3.58, LBR20 before 2.6.3.50, R7800 before 1.0.2.80, R8900 before 1.0.5.26, R9000 before 1.0.5.26, RBS50Y before 2.7.3.22, WNR2000v5 before 1.0.0.76, XR700 before 1.0.1.36, EX6150v2 before 1.0.1.98, EX7300 before 1.0.2.158, EX7320 before 1.0.0.134, RAX10 before 1.0.2.88, RAX120 before 1.2.0.16, RAX70 before 1.0.2.88, EX6100v2 before 1.0.1.98, EX6400 before 1.0.2.158, EX7300v2 before 1.0.0.134, R6700AX before 1.0.2.88, RAX120v2 before 1.2.0.16, RAX78 before 1.0.2.88, EX6410 before 1.0.0.134, RBR10 before 2.7.3.22, RBR20 before 2.7.3.22, RBR350 before 4.3.4.7, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, EX6420 before 1.0.0.134, RBS10 before 2.7.3.22, RBS20 before 2.7.3.22, RBS350 before 4.3.4.7, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, EX6400v2 before 1.0.0.134, RBK12 before 2.7.3.22, RBK20 before 2.7.3.22, RBK352 before 4.3.4.7, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	9.6	More Details
CVE-2021-45620	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, LAX20 before 1.1.6.28, MR60 before 1.0.6.116, MR80 before 1.1.2.20, MS60 before 1.0.6.116, MS80 before 1.1.2.20, MK62 before 1.0.6.116, MK83 before 1.1.2.20, R6400 before 1.0.1.70, R6400v2 before 1.0.4.106, R6700v3 before 1.0.4.106, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7850 before 1.0.5.74, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45621	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 3.2.18.2, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, EX3700 before 1.0.0.94, EX3800 before 1.0.0.94, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7000 before 1.0.1.104, EX7500 before 1.0.0.74, LAX20 before 1.1.6.28, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6300v2 before 1.0.4.52, R6400 before 1.0.1.70, R6400v2 before 1.0.4.106, R6700v3 before 1.0.4.106, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7100LG before 1.0.0.72, R7850 before 1.0.5.74, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, R8300 before 1.0.2.154, R8500 before 1.0.2.154, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	9.6	More Details
CVE-2021-45622	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, EX7500 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6400 before 1.0.1.70, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.116, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.38, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	9.6	More Details
CVE-2021-45624	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, R7000 before 1.0.11.110, R7100LG before 1.0.0.72, R7900 before 1.0.4.30, R8000 before 1.0.4.62, XR300 before 1.0.3.56, R7000P before 1.3.2.132, R8500 before 1.0.2.144, R6900P before 1.3.2.132, and R8300 before 1.0.2.144.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45625	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects XR300 before 1.0.3.68, R7000P before 1.3.3.140, and R6900P before 1.3.3.140.	9.6	More Details
CVE-2021-45631	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45626	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK20 before 2.6.1.36, RBR20 before 2.6.1.36, RBS20 before 2.6.1.38, RBK40 before 2.6.1.36, RBR40 before 2.6.1.36, RBS40 before 2.6.1.38, RBK50 before 2.6.1.40, RBR50 before 2.6.1.40, RBS50 before 2.6.1.40, and RBS50Y before 2.6.1.40.	9.6	More Details
CVE-2021-45502	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45629	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details
CVE-2021-45628	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 3.2.18.2, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBS40V before 2.6.2.4, and RBW30 before 2.6.2.2.	9.6	More Details
CVE-2021-45627	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45501	Certain NETGEAR devices are affected by authentication bypass. This affects AC2400 before 1.1.0.84, AC2600 before 1.1.0.84, D7000 before 1.0.1.82, R6020 before 1.0.0.52, R6080 before 1.0.0.52, R6120 before 1.0.0.80, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.84, R6330 before 1.1.0.84, R6350 before 1.1.0.84, R6700v2 before 1.1.0.84, R6800 before 1.1.0.84, R6850 before 1.1.0.84, R6900v2 before 1.1.0.84, R7200 before 1.1.0.84, R7350 before 1.1.0.84, R7400 before 1.1.0.84, and R7450 before 1.1.0.84.	9.4	More Details
CVE-2021-45497	NETGEAR D7000 devices before 1.0.1.82 are affected by authentication bypass.	9.4	More Details
CVE-2021-21877	Specially-crafted HTTP requests can lead to arbitrary command execution in “GET” requests. An attacker can make authenticated HTTP requests to trigger this vulnerability.	9.1	More Details
CVE-2021-21884	An OS command injection vulnerability exists in the Web Manager SslGenerateCSR functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21875	A specially-crafted HTTP request can lead to arbitrary command execution in EC keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21874	A specially-crafted HTTP request can lead to arbitrary command execution in DSA keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21873	A specially-crafted HTTP request can lead to arbitrary command execution in RSA keypasswd parameter. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-45496	NETGEAR D7000 devices before 1.0.1.82 are affected by authentication bypass.	9.1	More Details
CVE-2020-20944	An issue in /admin/index.php?lfj=mysql&action=del of Qibosoft v7 allows attackers to arbitrarily delete files.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21887	A stack-based buffer overflow vulnerability exists in the Web Manager SslGenerateCSR functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21888	An OS command injection vulnerability exists in the Web Manager SslGenerateCertificate functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21890	A stack-based buffer overflow vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution in the vulnerable portion of the branch (deletedir). An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21891	A stack-based buffer overflow vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to remote code execution in the vulnerable portion of the branch (deletefile). An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-21894	A directory traversal vulnerability exists in the Web Manager FsTFtp functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary file overwrite FsTFtp file disclosure. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.1	More Details
CVE-2021-45650	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R7000 before 1.0.11.110, R7900 before 1.0.4.30, R8000 before 1.0.4.62, RS400 before 1.5.1.80, R6400v2 before 1.0.4.102, R7000P before 1.3.2.126, R6700v3 before 1.0.4.102, and R6900P before 1.3.2.126.	9.1	More Details
CVE-2020-22057	The WinRin0x64.sys and WinRing0.sys low-level drivers in EVGA Precision XOC version v6.2.7 were discovered to be configured with the default security descriptor which allows attackers to access sensitive components and data.	9.1	More Details
CVE-2021-43985	An unauthenticated remote attacker can access mySCADA myPRO Versions 8.20.0 and prior without any form of authentication or authorization.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21876	Specially-crafted HTTP requests can lead to arbitrary command execution in PUT requests. An attacker can make authenticated HTTP requests to trigger this vulnerability.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-4144	TP-Link wifi router TL-WR802N V4(JP), with firmware version prior to 211202, is vulnerable to OS command injection.	8.8	More Details
CVE-2021-4168	showdoc is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2021-4067	Use after free in window manager in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-38008	Use after free in media in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-38007	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-38006	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-38005	Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4078	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4079	Out of bounds write in WebRTC in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via crafted WebRTC packets.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45337	Privilege escalation vulnerability in the Self-Defense driver of Avast Antivirus prior to 20.8 allows a local user with SYSTEM privileges to gain elevated privileges by "hollowing" process wsc_proxy.exe which could lead to acquire antimalware (AM-PPL) protection.	8.8	More Details
CVE-2021-21936	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'health_alt_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	8.8	More Details
CVE-2021-3621	A flaw was found in SSSD, where the sssctl command was vulnerable to shell command injection via the logs-fetch and cache-expire subcommands. This flaw allows an attacker to trick the root user into running a specially crafted sssctl command, such as via sudo, to gain root access. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	8.8	More Details
CVE-2021-21917	An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at ''ord' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	8.8	More Details
CVE-2021-21916	An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'description_filter' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	8.8	More Details
CVE-2021-21915	An exploitable SQL injection vulnerability exist in the 'group_list' page of the Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted HTTP request at 'company_filter' parameter. An attacker can make authenticated HTTP requests to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	8.8	More Details
CVE-2021-45335	Sandbox component in Avast Antivirus prior to 20.4 has an insecure permission which could be abused by local user to control the outcome of scans, and therefore evade detection or delete arbitrary system files.	8.8	More Details
CVE-2021-38011	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-38012	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38014	Out of bounds write in Swiftshader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-38015	Inappropriate implementation in input in Google Chrome prior to 96.0.4664.45 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	8.8	More Details
CVE-2021-38016	Insufficient policy enforcement in background fetch in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	8.8	More Details
CVE-2021-38017	Insufficient policy enforcement in iframe sandbox in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	8.8	More Details
CVE-2021-4066	Integer underflow in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4065	Use after free in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4064	Use after free in screen capture in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4063	Use after free in developer tools in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4062	Heap buffer overflow in BFCache in Google Chrome prior to 96.0.4664.93 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4052	Use after free in web apps in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2021-4053	Use after free in UI in Google Chrome on Linux prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4061	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4055	Heap buffer overflow in extensions in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.	8.8	More Details
CVE-2021-4056	Type confusion in loader in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4057	Use after free in file API in Google Chrome prior to 96.0.4664.93 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-45336	Privilege escalation vulnerability in the Sandbox component of Avast Antivirus prior to 20.4 allows a local sandboxed code to gain elevated privileges by using system IPC interfaces which could lead to exit the sandbox and acquire SYSTEM privileges.	8.8	More Details
CVE-2021-4058	Heap buffer overflow in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-21236	A vulnerability in /damicms-master/admin.php?s=/Article/doedit of DamiCMS v6.0 allows attackers to compromise and impersonate user accounts via obtaining a user's session cookie.	8.8	More Details
CVE-2021-21882	An OS command injection vulnerability exists in the Web Manager FsUnmount functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2021-21879	A directory traversal vulnerability exists in the Web Manager File Upload functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary file overwrite. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2021-21901	A stack-based buffer overflow vulnerability exists in the CMA check_udp_crc function of Garrett Metal Detectors' iC Module CMA Version 5.0. A specially-crafted packet can lead to a stack-based buffer overflow during a call to memcpy. An attacker can send a malicious packet to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20945	A Cross-Site Request Forgery (CSRF) in /admin/index.php?lfj=member&action=editmember of Qibosoft v7 allows attackers to arbitrarily add administrator accounts.	8.8	More Details
CVE-2021-43858	MinIO is a Kubernetes native application for cloud storage. Prior to version `RELEASE.2021-12-27T07-23-18Z`, a malicious client can hand-craft an HTTP API call that allows for updating policy for a user and gaining higher privileges. The patch in version `RELEASE.2021-12-27T07-23-18Z` changes the accepted request body type and removes the ability to apply policy changes through this API. There is a workaround for this vulnerability: Changing passwords can be disabled by adding an explicit `Deny` rule to disable the API for users.	8.8	More Details
CVE-2021-45418	Certain Starcharge products are vulnerable to Directory Traversal via main.cgi. The affected products include: Nova 360 Cabinet <=1.3.0.0.6 - Fixed: 1.3.0.0.9 and Titan 180 Premium <=1.3.0.0.7b102 - Fixed: Beta1.3.0.1.0.	8.8	More Details
CVE-2021-43630	Projectworlds Hospital Management System v1.0 is vulnerable to SQL injection via multiple parameters in add_patient.php. As a result, an authenticated malicious user can compromise the databases system and in some cases leverage this vulnerability to get remote code execution on the remote web server.	8.8	More Details
CVE-2021-45896	Nokia FastMile 3TG00118ABAD52 devices allow privilege escalation by an authenticated user via is_ctc_admin=1 to login_web_app.cgi and use of Import Config File.	8.8	More Details
CVE-2018-17875	A remote code execution issue in the ping command on Poly Trio 8800 5.7.1.4145 devices allows remote authenticated users to execute commands via unspecified vectors.	8.8	More Details
CVE-2021-45419	Certain Starcharge products are affected by Improper Input Validation. The affected products include: Nova 360 Cabinet <= 1.3.0.0.7b102 - Fixed: Beta1.3.0.1.0 and Titan 180 Premium <= 1.3.0.0.6 - Fixed: 1.3.0.0.9.	8.8	More Details
CVE-2021-45553	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7000 before 1.0.11.126, R6900P before 1.3.2.126, and R7000P before 1.3.2.126.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43853	Ajax.NET Professional (AjaxPro) is an AJAX framework available for Microsoft ASP.NET. Affected versions of this package are vulnerable to JavaScript object injection which may result in cross site scripting when leveraged by a malicious user. The affected core relates to JavaScript object creation when parsing json input. Releases before version 21.12.22.1 are affected. A workaround exists that replaces one of the core JavaScript files embedded in the library. See the GHSA-5q7q-qqw2-hjq7 for workaround details.	8.7	More Details
CVE-2021-45512	Certain NETGEAR devices are affected by weak cryptography. This affects D7000v2 before 1.0.0.62, D8500 before 1.0.3.50, EX3700 before 1.0.0.84, EX3800 before 1.0.0.84, EX6120 before 1.0.0.54, EX6130 before 1.0.0.36, EX7000 before 1.0.1.90, R6250 before 1.0.4.42, R6400v2 before 1.0.4.98, R6700v3 before 1.0.4.98, R6900P before 1.3.2.124, R7000 before 1.0.11.106, R7000P before 1.3.2.124, R7100LG before 1.0.0.56, R7900 before 1.0.4.26, R8000 before 1.0.4.58, R8300 before 1.0.2.134, R8500 before 1.0.2.134, RS400 before 1.5.0.48, WNR3500Lv2 before 1.2.0.62, and XR300 before 1.0.3.50.	8.6	More Details
CVE-2021-45536	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45596	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45597	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45598	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45599	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45544	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45542	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45558	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45555	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7900P before 1.4.2.84, R7960P before 1.4.2.84, and R8000P before 1.4.2.84.	8.4	More Details
CVE-2021-45554	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6400 before 1.0.1.74, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R7000 before 1.0.11.126, R6900P before 1.3.3.140, R7000P before 1.3.3.140, and R8000 before 1.0.4.74.	8.4	More Details
CVE-2021-45541	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7900 before 1.0.4.38, R7900P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX200 before 1.0.3.106, MR60 before 1.0.6.110, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45549	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects LAX20 before 1.1.6.28, MK62 before 1.1.6.122, MR60 before 1.1.6.122, MS60 before 1.1.6.122, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.116, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.38, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RS400 before 1.5.1.80, and XR1000 before 1.0.0.58.	8.4	More Details
CVE-2021-45535	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX200 before 1.0.3.106, RAX80 before 1.0.3.106, RAX75 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45540	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7000 before 1.0.11.126, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.3.106, MR60 before 1.0.6.110, RAX45 before 1.0.2.66, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX50 before 1.0.2.66, and RAX75 before 1.0.3.106.	8.4	More Details
CVE-2021-45600	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45547	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45539	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, MR60 before 1.0.6.110, RAX20 before 1.0.2.82, RAX45 before 1.0.2.28, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX50 before 1.0.2.28, and RAX75 before 1.0.3.106.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45538	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45594	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS50Y before 2.7.3.22, RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	8.4	More Details
CVE-2021-45546	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45545	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details
CVE-2021-45533	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects EX6120 before 1.0.0.66, EX6130 before 1.0.0.46, EX7000 before 1.0.1.106, EX7500 before 1.0.1.76, EX3700 before 1.0.0.94, EX3800 before 1.0.0.94, RBR850 before 4.6.3.9, RBS850 before 4.6.3.9, and RBK852 before 4.6.3.9.	8.4	More Details
CVE-2021-45537	Certain NETGEAR devices are affected by command injection by an authenticated user . This affects RAX200 before 1.0.3.106, RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45563	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45591	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45593	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.2.102, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBR50 before 2.7.2.102, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.2.102.	8.4	More Details
CVE-2021-45560	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45575	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45574	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45572	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45571	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45570	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45569	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45561	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45592	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45568	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45567	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45566	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45565	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45562	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45494	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	8.4	More Details
CVE-2021-45601	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45577	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45578	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45579	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45580	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45581	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45582	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45559	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45583	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45584	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45585	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45586	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45587	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45588	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45589	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45590	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45564	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45576	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	8.4	More Details
CVE-2021-45543	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R8000 before 1.0.4.74, RAX200 before 1.0.4.120, R8000P before 1.4.2.84, R7900P before 1.4.2.84, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and RBK852 before 3.2.17.12.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45679	Certain NETGEAR devices are affected by privilege escalation. This affects R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, and RS400 before 1.5.1.80.	8.4	More Details
CVE-2021-45623	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects R7800 before 1.0.2.74, R9000 before 1.0.5.2, and XR500 before 2.3.2.66.	8.3	More Details
CVE-2021-45637	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6260 before 1.1.0.76, R6800 before 1.2.0.62, R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, and AC2600 before 1.2.0.62.	8.3	More Details
CVE-2021-45573	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6260 before 1.1.0.76, R6800 before 1.2.0.62, R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, and AC2600 before 1.2.0.62.	8.3	More Details
CVE-2021-37563	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds write).	8.2	More Details
CVE-2021-37569	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds write).	8.2	More Details
CVE-2021-37568	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds write).	8.2	More Details
CVE-2021-37567	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds read).	8.2	More Details
CVE-2021-37566	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7610, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds write).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37565	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds read).	8.2	More Details
CVE-2021-37564	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds read).	8.2	More Details
CVE-2021-37561	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds write).	8.2	More Details
CVE-2021-37562	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds read).	8.2	More Details
CVE-2021-37571	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds write).	8.2	More Details
CVE-2021-37560	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds write).	8.2	More Details
CVE-2021-35055	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds write).	8.2	More Details
CVE-2021-32469	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915 Affected Software Versions 7.4.0.0; Out-of-bounds read).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32468	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds read).	8.2	More Details
CVE-2021-32467	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds read).	8.2	More Details
CVE-2021-37570	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds read).	8.2	More Details
CVE-2021-37572	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Missing authorization).	8.2	More Details
CVE-2021-43856	Wiki.js is a wiki app built on Node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through non-image file uploads for file types that can be viewed directly inline in the browser. By creating a malicious file which can execute inline JS when viewed in the browser (e.g. XML files), a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the file is viewed directly by other users. The file must be opened directly by the user and will not trigger directly in a normal Wiki.js page. A patch in version 2.5.264 fixes this vulnerability by adding an optional (enabled by default) force download flag to all non-image file types, preventing the file from being viewed inline in the browser. As a workaround, disable file upload for all non-trusted users. --- Thanks to @Haxatron for reporting this vulnerability. Initially reported via https://huntr.dev/bounties/266bff09-00d9-43ca-a4bb-bb540642811f/	8.2	More Details
CVE-2021-37584	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol. (Affected Chipsets MT7603E, MT7610, MT7612, MT7613, MT7615, MT7620, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0; Out-of-bounds write).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23175	NVIDIA GeForce Experience contains a vulnerability in user authorization, where GameStream does not correctly apply individual user access controls for users on the same device, which, with user intervention, may lead to escalation of privileges, information disclosure, data tampering, and denial of service, affecting other resources beyond the intended security authority of GameStream.	8.2	More Details
CVE-2021-45643	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, and XR1000 before 1.0.0.58.	8.2	More Details
CVE-2021-45499	Certain NETGEAR devices are affected by authentication bypass. This affects R6900P before 1.3.3.140, R7000P before 1.3.3.140, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000P before 1.4.2.84, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	8.2	More Details
CVE-2021-45510	NETGEAR XR1000 devices before 1.0.0.58 are affected by authentication bypass.	8.2	More Details
CVE-2021-43845	PJSIP is a free and open source multimedia communication library. In version 2.11.1 and prior, if incoming RTCP XR message contain block, the data field is not checked against the received packet size, potentially resulting in an out-of-bound read access. This affects all users that use PJMEDIA and RTCP XR. A malicious actor can send a RTCP XR message with an invalid packet size.	8.2	More Details
CVE-2021-43855	Wiki.js is a wiki app built on node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through a SVG file upload made via a custom request with a fake MIME type. By creating a crafted SVG file, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the SVG is viewed directly by other users. Scripts do not execute when loaded inside a page via normal `<img>` tags. The malicious SVG can only be uploaded by crafting a custom request to the server with a fake MIME type. A patch in version 2.5.264 fixes this vulnerability by adding an additional file extension verification check to the optional (enabled by default) SVG sanitization step to all file uploads that match the SVG mime type. As a workaround, disable file upload for all non-trusted users.	8.2	More Details
CVE-2021-37583	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols. (Affected Chipsets MT7603E, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 2.0.2; Out-of-bounds write).	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45645	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects RBS50Y before 2.7.0.122, SRK60 before 2.7.0.122, SRR60 before 2.7.0.122, SRS60 before 2.7.0.122, SXK30 before 3.2.33.108, SXR30 before 3.2.33.108, SXS30 before 3.2.33.108, and SRC60 before 2.7.0.122.	8.2	More Details
CVE-2021-45528	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R6300v2 before 1.0.4.52, R6400 before 1.0.1.52, R6900 before 1.0.2.8, R7000 before 1.0.9.88, R7900 before 1.0.3.18, R8000 before 1.0.4.46, R7900P before 1.4.1.50, R8000P before 1.4.1.50, RAX75 before 1.0.3.88, RAX80 before 1.0.3.88, and WNR3500Lv2 before 1.2.0.62.	8.1	More Details
CVE-2021-36750	ENC DataVault before 7.2 and VaultAPI v67 mishandle key derivation, making it easier for attackers to determine the passwords of all DataVault users (across USB drives sold under multiple brand names).	8.1	More Details
CVE-2021-45710	An issue was discovered in the tokio crate before 1.8.4, and 1.9.x through 1.13.x before 1.13.1, for Rust. In certain circumstances involving a closed oneshot channel, there is a data race and memory corruption.	8.1	More Details
CVE-2021-20873	Yappli is an application development platform which provides the function to access a requested URL using Custom URL Scheme. When Android apps are developed with Yappli versions since v7.3.6 and prior to v9.30.0, they are vulnerable to improper authorization in Custom URL Scheme handler, and may be directed to unintended sites via a specially crafted URL.	8.1	More Details
CVE-2021-21953	An authentication bypass vulnerability exists in the process_msg() function of the home_security binary of Anker Eufy Homebase 2 2.1.6.9h. A specially-crafted man-in-the-middle attack can lead to increased privileges.	8.1	More Details
CVE-2021-33017	The standard access path of the IntelliBridge EC 40 and 60 Hub (C.00.04 and prior) requires authentication, but the product has an alternate path or channel that does not require authentication.	8.1	More Details
CVE-2021-32993	IntelliBridge EC 40 and 60 Hub (C.00.04 and prior) contains hard-coded credentials, such as a password or a cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21751	ZTE BigVideo analysis product has an input verification vulnerability. Due to the inconsistency between the front and back verifications when configuring the large screen page, an attacker with high privileges could exploit this vulnerability to tamper with the URL and cause service exception.	8.1	More Details
CVE-2021-21902	An authentication bypass vulnerability exists in the CMA run_server_6877 functionality of Garrett Metal Detectors iC Module CMA Version 5.0. A properly-timed network connection can lead to authentication bypass via session hijacking. An attacker can send a sequence of requests to trigger this vulnerability.	8.1	More Details
CVE-2021-21909	Specially-crafted command line arguments can lead to arbitrary file deletion in the del .cntl.log file delete command. An attacker can provide malicious inputs to trigger this vulnerability	8.1	More Details
CVE-2021-45704	An issue was discovered in the metrics-util crate before 0.7.0 for Rust. There is a data race and memory corruption because AtomicBucket<T> unconditionally implements the Send and Sync traits.	8.1	More Details
CVE-2021-43851	Anuko Time Tracker is an open source, web-based time tracking application written in PHP. SQL injection vulnerability exist in multiple files in Time Tracker version 1.19.33.5606 and prior due to not properly checking of the "group" and "status" parameters in POST requests. Group parameter is posted along when navigating between organizational subgroups (groups.php file). Status parameter is used in multiple files to change a status of an entity such as making a project, task, or user inactive. This issue has been patched in version 1.19.33.5607. An upgrade is highly recommended. If an upgrade is not practical, introduce ttValidStatus function as in the latest version and start using it user input check blocks wherever status field is used. For groups.php fix, introduce ttValidInteger function as in the latest version and use it in the access check block in the file.	8.1	More Details
CVE-2021-44078	An issue was discovered in split_region in uc.c in Unicorn Engine before 2.0.0-rc5. It allows local attackers to escape the sandbox. An attacker must first obtain the ability to execute crafted code in the target sandbox in order to exploit this vulnerability. The specific flaw exists within the virtual memory manager. The issue results from the faulty comparison of GVA and GPA while calling uc_mem_map_ptr to free part of a claimed memory block. An attacker can leverage this vulnerability to escape the sandbox and execute arbitrary code on the host machine.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13905	A race condition was addressed with additional validation. This issue is fixed in tvOS 11.2, iOS 11.2, macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan, watchOS 4.2. An application may be able to gain elevated privileges.	8.1	More Details
CVE-2020-20593	A cross-site request forgery (CSRF) in Rockoa v1.9.8 allows an authenticated attacker to arbitrarily add an administrator account.	8.0	More Details
CVE-2021-45649	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6400v2 before 1.0.4.84, R6700v3 before 1.0.4.84, R7000 before 1.0.11.126, R6900P before 1.3.2.126, and R7000P before 1.3.2.126.	7.9	More Details
CVE-2017-13906	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan, macOS High Sierra 10.13. A malicious application may be able to elevate privileges.	7.8	More Details
CVE-2021-21911	A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-40160	PDFTron prior to 9.0.7 version may be forced to read beyond allocated boundaries when parsing a maliciously crafted PDF file. This vulnerability can be exploited to execute arbitrary code.	7.8	More Details
CVE-2021-45463	load_cache in GEGL before 0.4.34 allows shell expansion when a pathname in a constructed command line is not escaped or filtered. This is caused by use of the system library function for execution of the ImageMagick convert fallback in magick-load. NOTE: GEGL releases before 0.4.34 are used in GIMP releases before 2.10.30; however, this does not imply that GIMP builds enable the vulnerable feature.	7.8	More Details
CVE-2021-4173	vim is vulnerable to Use After Free	7.8	More Details
CVE-2021-21912	A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45339	Privilege escalation vulnerability in Avast Antivirus prior to 20.4 allows a local user to gain elevated privileges by "hollowing" trusted process which could lead to the bypassing of Avast self-defense.	7.8	More Details
CVE-2021-45338	Multiple privilege escalation vulnerabilities in Avast Antivirus prior to 20.4 allow a local user to gain elevated privileges by calling unnecessarily powerful internal methods of the main antivirus service which could lead to the (1) arbitrary file delete, (2) write and (3) reset security.	7.8	More Details
CVE-2018-4302	A null pointer dereference was addressed with improved validation. This issue is fixed in macOS High Sierra 10.13, iCloud for Windows 7.0, watchOS 4, iOS 11, iTunes 12.7 for Windows. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-21910	A privilege escalation vulnerability exists in the Windows version of installation for Advantech R-SeeNet Advantech R-SeeNet 2.4.15 (30.07.2021). A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-23244	ColorOS pregrant dangerous permissions to apps which are listed in a whitelist xml named default-grant-permissions.But some apps in whitelist is not installed, attacker can disguise app with the same package name to obtain dangerous permission.	7.8	More Details
CVE-2017-13908	An issue in handling file permissions was addressed with improved validation. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan, macOS High Sierra 10.13. A local attacker may be able to execute non-executable text files via an SMB share.	7.8	More Details
CVE-2021-4118	pytorch-lightning is vulnerable to Deserialization of Untrusted Data	7.8	More Details
CVE-2017-13880	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 11.2, watchOS 4.2. An application may be able to execute arbitrary code with kernel privilege.	7.8	More Details
CVE-2017-13835	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS High Sierra 10.13. An application may be able to execute arbitrary code with elevated privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45469	In __f2fs_setxattr in fs/f2fs/xattr.c in the Linux kernel through 5.15.11, there is an out-of-bounds memory access when an inode has an invalid last xattr entry.	7.8	More Details
CVE-2020-3886	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-21750	ZTE BigVideo Analysis product has a privilege escalation vulnerability. Due to improper management of the timed task modification privilege, an attacker with ordinary user permissions could exploit this vulnerability to gain unauthorized access.	7.8	More Details
CVE-2021-45908	An issue was discovered in gif2apng 1.9. There is a stack-based buffer overflow involving a while loop. An attacker has little influence over the data written to the stack, making it unlikely that the flow of control can be subverted.	7.8	More Details
CVE-2021-45907	An issue was discovered in gif2apng 1.9. There is a stack-based buffer overflow involving a for loop. An attacker has little influence over the data written to the stack, making it unlikely that the flow of control can be subverted.	7.8	More Details
CVE-2020-22061	SUPERAntispyware v8.0.0.1050 was discovered to contain an issue in the component saskutil64.sys. This issue allows attackers to arbitrarily write data to the device via IOCTL 0x9C402140.	7.8	More Details
CVE-2021-43556	FATEK WinProladder Versions 3.30_24518 and prior are vulnerable to a stack-based buffer overflow while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-43554	FATEK WinProladder Versions 3.30_24518 and prior are vulnerable to an out-of-bounds write while processing project files, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-45911	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow in the main function. It allows an attacker to write 2 bytes outside the boundaries of the buffer.	7.8	More Details
CVE-2021-45910	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow within the main function. It allows an attacker to write data outside of the allocated buffer. The attacker has control over a part of the address that data is written to, control over the written data, and (to some extent) control over the amount of data that is written.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45534	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects AC2100 before 1.2.0.88, AC2400 before 1.2.0.88, AC2600 before 1.2.0.88, D7000 before 1.0.1.82, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.84, R6330 before 1.1.0.84, R6350 before 1.1.0.84, R6700v2 before 1.2.0.88, R6800 before 1.2.0.88, R6850 before 1.1.0.84, R6900v2 before 1.2.0.88, R7200 before 1.2.0.88, R7350 before 1.2.0.88, R7400 before 1.2.0.88, and R7450 before 1.2.0.88.	7.8	More Details
CVE-2021-45909	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow vulnerability in the DecodeLZW function. It allows an attacker to write a large amount of arbitrary data outside the boundaries of a buffer.	7.8	More Details
CVE-2021-40161	A Memory Corruption vulnerability may lead to code execution through maliciously crafted DLL files through PDFTron earlier than 9.0.7 version.	7.8	More Details
CVE-2021-45524	NETGEAR R8000 devices before 1.0.4.62 are affected by a buffer overflow by an authenticated user.	7.6	More Details
CVE-2021-45551	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.42, R6080 before 1.0.0.42, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.64, R6800 before 1.2.0.62, R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, AC2600 before 1.2.0.62, and WNR2020 before 1.1.0.62.	7.6	More Details
CVE-2021-20826	Unprotected transport of credentials vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and earlier, FC6A Series MICROSmart Plus CPU module v1.91 and earlier, WindLDR v8.19.1 and earlier, WindEDIT Lite v1.3.1 and earlier, and Data File Manager v2.12.1 and earlier) allows an attacker to obtain the PLC Web server user credentials from the communication between the PLC and the software. As a result, the complete access privileges to the PLC Web server may be obtained, and manipulation of the PLC output and/or suspension of the PLC may be conducted.	7.6	More Details
CVE-2021-45493	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RAX35 before 1.0.4.102, RAX38 before 1.0.4.102, and RAX40 before 1.0.4.102.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45595	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects LBR20 before 2.6.3.50, RBS50Y before 2.7.3.22, RBR10 before 2.7.3.22, RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, RBS10 before 2.7.3.22, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, RBK12 before 2.7.3.22, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	7.6	More Details
CVE-2021-45713	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_scalar_function has a use-after-free.	7.5	More Details
CVE-2021-45712	An issue was discovered in the rust-embed crate before 6.3.0 for Rust. A ../ directory traversal can sometimes occur in debug mode.	7.5	More Details
CVE-2021-20049	A vulnerability in SonicWall SMA100 password change API allows a remote unauthenticated attacker to perform SMA100 username enumeration based on the server responses. This vulnerability impacts 10.2.1.2-24sv, 10.2.0.8-37sv and earlier 10.x versions.	7.5	More Details
CVE-2021-45642	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.64, EX6250 before 1.0.0.134, EX7700 before 1.0.0.222, LBR20 before 2.6.3.50, RBS50Y before 2.7.3.22, R8900 before 1.0.5.26, R9000 before 1.0.5.26, XR450 before 2.3.2.66, XR500 before 2.3.2.66, XR700 before 1.0.1.36, EX7320 before 1.0.0.134, RAX120 before 1.2.2.24, EX7300v2 before 1.0.0.134, RAX120v2 before 1.2.2.24, EX6410 before 1.0.0.134, RBR10 before 2.7.3.22, RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, EX6420 before 1.0.0.134, RBS10 before 2.7.3.22, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, EX6400v2 before 1.0.0.134, RBK12 before 2.7.3.22, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	7.5	More Details
CVE-2021-45266	A null pointer dereference vulnerability exists in gpac 1.1.0 via the lsr_read_anim_values_ex function, which causes a segmentation fault and application crash.	7.5	More Details
CVE-2021-42583	A Broken or Risky Cryptographic Algorithm exists in Max Mazurov Maddy before 0.5.2, which is an unnecessary risk that may result in the exposure of sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43854	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. Versions prior to 3.6.5 are vulnerable to regular expression denial of service (ReDoS) attacks. The vulnerability is present in PunktSentenceTokenizer, sent_tokenize and word_tokenize. Any users of this class, or these two functions, are vulnerable to the ReDoS attack. In short, a specifically crafted long input to any of these vulnerable functions will cause them to take a significant amount of execution time. If your program relies on any of the vulnerable functions for tokenizing unpredictable user input, then we would strongly recommend upgrading to a version of NLTK without the vulnerability. For users unable to upgrade the execution time can be bounded by limiting the maximum length of an input to any of the vulnerable functions. Our recommendation is to implement such a limit.	7.5	More Details
CVE-2021-45715	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_window_function has a use-after-free.	7.5	More Details
CVE-2021-20050	An Improper Access Control Vulnerability in the SMA100 series leads to multiple restricted management APIs being accessible without a user login, potentially exposing configuration meta-data.	7.5	More Details
CVE-2021-45714	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_aggregate_function has a use-after-free.	7.5	More Details
CVE-2021-44600	The password parameter on Simple Online Mens Salon Management System (MSMS) 1.0 appears to be vulnerable to SQL injection attacks through the password parameter. The predictive tests of this application interacted with that domain, indicating that the injected SQL query was executed. The attacker can retrieve all authentication and information about the users of this system.	7.5	More Details
CVE-2021-45462	In Open5GS 2.4.0, a crafted packet from UE can crash SGW-U/UPF.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45557	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TUP before 1.0.5.3, GS710TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS724TPP before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPP before 6.0.8.2, GS750E before 1.0.1.10, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	7.5	More Details
CVE-2021-45884	In Brave Desktop 1.17 through 1.33 before 1.33.106, when CNAME-based adblocking and a proxying extension with a SOCKS fallback are enabled, additional DNS requests are issued outside of the proxying extension using the system's DNS settings, resulting in information disclosure. NOTE: this issue exists because of an incomplete fix for CVE-2021-21323 and CVE-2021-22916.	7.5	More Details
CVE-2021-44599	The id parameter from Online Enrollment Management System 1.0 system appears to be vulnerable to SQL injection attacks. A crafted payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed. The attacker can retrieve sensitive information for all users of this system.	7.5	More Details
CVE-2020-20948	An arbitrary file download vulnerability in jeecg v3.8 allows attackers to access sensitive files via modification of the "localPath" variable.	7.5	More Details
CVE-2021-45556	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects GS108Tv2 before 5.4.2.36, GS110TPP before 7.0.7.2, GS110TPv2 before 5.4.2.36., GS110TPv3 before 7.0.7.2, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	7.5	More Details
CVE-2021-23228	DIAEnergie Version 1.7.5 and prior is vulnerable to a reflected cross-site scripting attack through error pages that are returned by “.NET Request.QueryString”.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13892	An issue existed in the handling of Contact sharing. This issue was addressed with improved handling of user information. This issue is fixed in macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan. Sharing contact information may lead to unexpected data sharing.	7.5	More Details
CVE-2019-25055	An issue was discovered in the libpulse-binding crate before 2.6.0 for Rust. It mishandles a panic that crosses a Foreign Function Interface (FFI) boundary.	7.5	More Details
CVE-2021-45700	An issue was discovered in the ckb crate before 0.40.0 for Rust. Attackers can cause a denial of service (Nervos CKB blockchain node crash) via a dead call that is used as a DepGroup.	7.5	More Details
CVE-2021-45699	An issue was discovered in the ckb crate before 0.40.0 for Rust. Remote attackers may be able to conduct a 51% attack against the Nervos CKB blockchain by triggering an inability to allocate memory for the misbehavior HashMap.	7.5	More Details
CVE-2021-45694	An issue was discovered in the rdiff crate through 2021-02-03 for Rust. Window may read from uninitialized memory locations.	7.5	More Details
CVE-2021-45681	An issue was discovered in the derive-com-impl crate before 0.1.2 for Rust. An invalid reference (and memory corruption) can occur because AddRef might not be called before returning a pointer.	7.5	More Details
CVE-2021-45680	An issue was discovered in the vec-const crate before 2.0.0 for Rust. It tries to construct a Vec from a pointer to a const slice, leading to memory corruption.	7.5	More Details
CVE-2021-45470	lib/DatabaseLayer.py in cve-search before 4.1.0 allows regular expression injection, which can lead to ReDoS (regular expression denial of service) or other impacts.	7.5	More Details
CVE-2020-36511	An issue was discovered in the bite crate through 2020-12-31 for Rust. read::BiteReadExpandedExt::read_framed_max may read from uninitialized memory locations.	7.5	More Details
CVE-2019-25054	An issue was discovered in the pnet crate before 0.27.2 for Rust. There is a segmentation fault (upon attempted dereference of an uninitialized descriptor) because of an erroneous IcmpTransportChannelIterator compiler optimization.	7.5	More Details
CVE-2021-45720	An issue was discovered in the lru crate before 0.7.1 for Rust. The iterators have a use-after-free, as demonstrated by an access after a pop operation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25028	An issue was discovered in the libpulse-binding crate before 1.2.1 for Rust. get_context can cause a use-after-free.	7.5	More Details
CVE-2021-44542	A memory leak vulnerability was found in Privoxy when handling errors.	7.5	More Details
CVE-2021-44541	A vulnerability was found in Privoxy which was fixed in process_encrypted_request_headers() by freeing header memory when failing to get the request destination.	7.5	More Details
CVE-2021-44540	A vulnerability was found in Privoxy which was fixed in get_url_spec_param() by freeing memory of compiled pattern spec before bailing.	7.5	More Details
CVE-2021-43989	mySCADA myPRO Versions 8.20.0 and prior stores passwords using MD5, which may allow an attacker to crack the previously retrieved password hashes.	7.5	More Details
CVE-2018-25027	An issue was discovered in the libpulse-binding crate before 1.2.1 for Rust. get_format_info can cause a use-after-free.	7.5	More Details
CVE-2018-25023	An issue was discovered in the smallvec crate before 0.6.13 for Rust. It can create an uninitialized value of any type, including a reference type.	7.5	More Details
CVE-2021-20827	Plaintext storage of a password vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and earlier, FC6A Series MICROSmart Plus CPU module v1.91 and earlier, WindLDR v8.19.1 and earlier, WindEDIT Lite v1.3.1 and earlier, and Data File Manager v2.12.1 and earlier) allows an attacker to obtain the PLC Web server user credentials from file servers, backup repositories, or ZLD files saved in SD cards. As a result, the attacker may access the PLC Web server and hijack the PLC, and manipulation of the PLC output and/or suspension of the PLC may be conducted.	7.5	More Details
CVE-2021-20874	Incorrect permission assignment for critical resource vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows a remote unauthenticated attacker to access arbitrary files on the server and obtain sensitive information via unspecified vectors.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45702	An issue was discovered in the tremor-script crate before 0.11.6 for Rust. A merge operation may result in a use-after-free.	7.5	More Details
CVE-2021-45719	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. update_hook has a use-after-free.	7.5	More Details
CVE-2021-45716	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_collation has a use-after-free.	7.5	More Details
CVE-2021-44544	DIAEnergie Version 1.7.5 and prior is vulnerable to multiple cross-site scripting vulnerabilities when arbitrary code is injected into the parameter “name” of the script “HandlerEnergyType.ashx”.	7.5	More Details
CVE-2021-44471	DIAEnergie Version 1.7.5 and prior is vulnerable to stored cross-site scripting when an unauthenticated user injects arbitrary code into the parameter “name” of the script “DIAE_HandlerAlarmGroup.ashx”.	7.5	More Details
CVE-2017-2488	A cryptographic weakness existed in the authentication protocol of Remote Desktop. This issue was addressed by implementing the Secure Remote Password authentication protocol. This issue is fixed in Apple Remote Desktop 3.9. An attacker may be able to capture cleartext passwords.	7.5	More Details
CVE-2021-45489	In NetBSD through 9.2, the IPv6 Flow Label generation algorithm employs a weak cryptographic PRNG.	7.5	More Details
CVE-2021-45488	In NetBSD through 9.2, there is an information leak in the TCP ISN (ISS) generation algorithm.	7.5	More Details
CVE-2021-45487	In NetBSD through 9.2, the IPv4 ID generation algorithm does not use appropriate cryptographic measures.	7.5	More Details
CVE-2021-45485	In the IPv6 implementation in the Linux kernel before 5.13.3, net/ipv6/output_core.c has an information leak because of certain use of a hash table which, although big, doesn't properly consider that IPv6-based attackers can typically choose among many IPv6 source addresses.	7.5	More Details
CVE-2021-45484	In NetBSD through 9.2, the IPv6 fragment ID generation algorithm employs a weak cryptographic PRNG.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24998	The Simple JWT Login WordPress plugin before 3.3.0 can be used to create new WordPress user accounts with a randomly generated password. The password is generated using the str_shuffle PHP function that "does not generate cryptographically secure values, and should not be used for cryptographic purposes" according to PHP's documentation.	7.5	More Details
CVE-2021-45711	An issue was discovered in the simple_asn1 crate 0.6.0 before 0.6.1 for Rust. There is a panic if UTCTime data, supplied by a remote attacker, has a second character greater than 0x7f.	7.5	More Details
CVE-2021-45717	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. commit_hook has a use-after-free.	7.5	More Details
CVE-2021-45718	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. rollback_hook has a use-after-free.	7.5	More Details
CVE-2021-23490	The package parse-link-header before 2.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the checkHeader function.	7.5	More Details
CVE-2021-45708	An issue was discovered in the abomonation crate through 2021-10-17 for Rust. Because transmute operations are insufficiently constrained, there can be an information leak or ASLR bypass.	7.5	More Details
CVE-2021-23772	This affects all versions of package github.com/kataras/iris; all versions of package github.com/kataras/iris/v12. The unsafe handling of file names during upload using UploadFormFiles method may enable attackers to write to arbitrary locations outside the designated target folder.	7.5	More Details
CVE-2021-23574	All versions of package js-data are vulnerable to Prototype Pollution via the deepFillIn and the set functions. This is an incomplete fix of [CVE-2020-28442](https://snyk.io/vuln/SNYK-JS-JSDATA-1023655).	7.5	More Details
CVE-2021-45651	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK50 before 2.7.3.22, RBR50 before 2.7.3.22, and RBS50 before 2.7.3.22.	7.4	More Details
CVE-2021-45521	Certain NETGEAR devices are affected by a hardcoded password. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44273	e2guardian v5.4.x <= v5.4.3r is affected by missing SSL certificate validation in the SSL MITM engine. In standalone mode (i.e., acting as a proxy or a transparent proxy), with SSL MITM enabled, e2guardian, if built with OpenSSL v1.1.x, did not validate hostnames in certificates of the web servers that it connected to, and thus was itself vulnerable to MITM attacks.	7.4	More Details
CVE-2021-45529	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects CBR40 before 2.3.5.12, D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, R6400 before 1.0.1.70, R7000 before 1.0.11.126, R6900P before 1.3.2.124, R7000P before 1.3.2.124, R7900 before 1.0.4.30, R8000 before 1.0.4.52, and WNR3500Lv2 before 1.2.0.62.	7.3	More Details
CVE-2021-37706	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In affected versions if the incoming STUN message contains an ERROR-CODE attribute, the header length is not checked before performing a subtraction operation, potentially resulting in an integer underflow scenario. This issue affects all users that use STUN. A malicious actor located within the victim's network may forge and send a specially crafted UDP (STUN) message that could remotely execute arbitrary code on the victim's machine. Users are advised to upgrade as soon as possible. There are no known workarounds.	7.3	More Details
CVE-2021-45526	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects EX6000 before 1.0.0.38, EX6120 before 1.0.0.48, EX6130 before 1.0.0.30, R6300v2 before 1.0.4.52, R6400 before 1.0.1.52, R7000 before 1.0.11.126, R7900 before 1.0.4.30, R8000 before 1.0.4.52, R7000P before 1.3.2.124, R8000P before 1.4.1.50, RAX80 before 1.0.3.88, R6900P before 1.3.2.124, R7900P before 1.4.1.50, and RAX75 before 1.0.3.88.	7.3	More Details
CVE-2021-43804	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In affected versions if the incoming RTCP BYE message contains a reason's length, this declared length is not checked against the actual received packet size, potentially resulting in an out-of-bound read access. This issue affects all users that use PJMEDIA and RTCP. A malicious actor can send a RTCP BYE message with an invalid reason length. Users are advised to upgrade as soon as possible. There are no known workarounds.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20318	The HornetQ component of Artemis in EAP 7 was not updated with the fix for CVE-2016-4978. A remote attacker could use this flaw to execute arbitrary code with the permissions of the application using a JMS ObjectMessage.	7.2	More Details
CVE-2021-21895	A directory traversal vulnerability exists in the Web Manager FsTFtp functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to FsTFtp file overwrite. An attacker can make an authenticated HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2021-3584	A server side remote code execution vulnerability was found in Foreman project. A authenticated attacker could use Sendmail configuration options to overwrite the defaults and perform command injection. The highest threat from this vulnerability is to confidentiality, integrity and availability of system. Fixed releases are 2.4.1, 2.5.1, 3.0.0.	7.2	More Details
CVE-2021-24753	The Rich Reviews by Starfish WordPress plugin before 1.9.6 does not properly validate the orderby GET parameter of the pending reviews page before using it in a SQL statement, leading to an authenticated SQL injection issue	7.2	More Details
CVE-2021-21905	Stack-based buffer overflow vulnerability exists in how the CMA readfile function of Garrett Metal Detectors iC Module CMA Version 5.0 is used at various locations. The Garrett iC Module exposes an authenticated CLI over TCP port 6877. This interface is used by a secondary GUI client, called “CMA Connect”, to interact with the iC Module on behalf of the user. After a client successfully authenticates, they can send plaintext commands to manipulate the device.	7.2	More Details
CVE-2021-21904	A directory traversal vulnerability exists in the CMA CLI setenv command of Garrett Metal Detectors’ iC Module CMA Version 5.0. An attacker can provide malicious input to trigger this vulnerability	7.2	More Details
CVE-2021-21906	Stack-based buffer overflow vulnerability exists in how the CMA readfile function of Garrett Metal Detectors iC Module CMA Version 5.0 is used at various locations. The Garrett iC Module exposes an authenticated CLI over TCP port 6877. This interface is used by a secondary GUI client, called “CMA Connect”, to interact with the iC Module on behalf of the user. Every time a user submits a password to the CLI password prompt, the buffer containing their input is passed as the password parameter to the checkPassword function.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21885	A directory traversal vulnerability exists in the Web Manager FsMove functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially crafted HTTP request can lead to local file inclusion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2021-21880	A directory traversal vulnerability exists in the Web Manager FsCopyFile functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to local file inclusion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	7.2	More Details
CVE-2021-45531	NETGEAR D6220 devices before 1.0.0.76 are affected by command injection by an authenticated user.	7.1	More Details
CVE-2021-45661	Certain NETGEAR devices are affected by server-side injection. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	7.1	More Details
CVE-2021-45660	Certain NETGEAR devices are affected by server-side injection. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	7.1	More Details
CVE-2021-4166	vim is vulnerable to Out-of-bounds Read	7.1	More Details
CVE-2021-45659	Certain NETGEAR devices are affected by server-side injection. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45658	Certain NETGEAR devices are affected by server-side injection. This affects D7800 before 1.0.1.58, DM200 before 1.0.0.66, EX2700 before 1.0.1.56, EX6150v2 before 1.0.1.86, EX6100v2 before 1.0.1.86, EX6200v2 before 1.0.1.78, EX6250 before 1.0.0.110, EX6410 before 1.0.0.110, EX6420 before 1.0.0.110, EX6400v2 before 1.0.0.110, EX7300 before 1.0.2.144, EX6400 before 1.0.2.144, EX7320 before 1.0.0.110, EX7300v2 before 1.0.0.110, R7500v2 before 1.0.3.48, R7800 before 1.0.2.68, R8900 before 1.0.5.2, R9000 before 1.0.5.2, RAX120 before 1.0.1.90, RBK40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, RBS50Y before 2.6.1.40, WN3000RPv2 before 1.0.0.78, WN3000RPv3 before 1.0.2.80, WNR2000v5 before 1.0.0.72, XR500 before 2.3.2.56, and XR700 before 1.0.1.20.	7.1	More Details
CVE-2021-45657	Certain NETGEAR devices are affected by server-side injection. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, RBS50Y before 2.6.1.40, and WNR2020 before 1.1.0.62.	7.1	More Details
CVE-2021-45656	Certain NETGEAR devices are affected by server-side injection. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	7.1	More Details
CVE-2021-44733	A use-after-free exists in drivers/tee/tee_shm.c in the TEE subsystem in the Linux kernel through 5.15.11. This occurs because of a race condition in tee_shm_get_from_id during an attempt to free a shared memory object.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45516	Certain NETGEAR devices are affected by denial of service. This affects R6400 before 1.0.1.70, R7000 before 1.0.11.126, R6900P before 1.3.3.140, R7000P before 1.3.3.140, R8000 before 1.0.4.74, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	6.9	More Details
CVE-2021-45655	NETGEAR R6400 devices before 1.0.1.70 are affected by server-side injection.	6.9	More Details
CVE-2017-13907	A state management issue was addressed with improved state validation. This issue is fixed in macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan. The screen lock may unexpectedly remain unlocked.	6.8	More Details
CVE-2018-4478	A validation issue was addressed with improved logic. This issue is fixed in macOS High Sierra 10.13.5, Security Update 2018-003 Sierra, Security Update 2018-003 El Capitan. An attacker with physical access to a device may be able to elevate privileges.	6.8	More Details
CVE-2021-20876	Path traversal vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows an attacker with an administrative privilege to obtain sensitive information stored in the hierarchy above the directory on the published site's server via unspecified vectors.	6.8	More Details
CVE-2021-45511	Certain NETGEAR devices are affected by authentication bypass. This affects AC2100 before 2021-08-27, AC2400 before 2021-08-27, AC2600 before 2021-08-27, D7000 before 2021-08-27, R6220 before 2021-08-27, R6230 before 2021-08-27, R6260 before 2021-08-27, R6330 before 2021-08-27, R6350 before 2021-08-27, R6700v2 before 2021-08-27, R6800 before 2021-08-27, R6850 before 2021-08-27, R6900v2 before 2021-08-27, R7200 before 2021-08-27, R7350 before 2021-08-27, R7400 before 2021-08-27, and R7450 before 2021-08-27.	6.8	More Details
CVE-2021-45607	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, RAX200 before 1.0.5.126, RAX75 before 1.0.5.126, and RAX80 before 1.0.5.126.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45644	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects AC2100 before 1.2.0.88, AC2400 before 1.2.0.88, AC2600 before 1.2.0.88, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.84, R6330 before 1.1.0.84, R6350 before 1.1.0.84, R6700v2 before 1.2.0.88, R6800 before 1.2.0.88, R6850 before 1.1.0.84, R6900v2 before 1.2.0.88, R7200 before 1.2.0.88, R7350 before 1.2.0.88, R7400 before 1.2.0.88, and R7450 before 1.2.0.88.	6.8	More Details
CVE-2021-35232	Hard coded credentials discovered in SolarWinds Web Help Desk product. Through these credentials, the attacker with local access to the Web Help Desk host machine allows to execute arbitrary HQL queries against the database and leverage the vulnerability to steal the password hashes of the users or insert arbitrary data into the database.	6.8	More Details
CVE-2021-35031	A vulnerability in the TFTP client of Zyxel GS1900 series firmware, XGS1210 series firmware, and XGS1250 series firmware, which could allow an authenticated LAN user to execute arbitrary OS commands via the GUI of the vulnerable device.	6.8	More Details
CVE-2021-45532	NETGEAR R8000 devices before 1.0.4.76 are affected by command injection by an authenticated user.	6.7	More Details
CVE-2021-44832	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.	6.6	More Details
CVE-2021-45550	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.78, D6100 before 1.0.0.63, D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DGN2200Bv4 before 1.0.0.109, DGN2200v4 before 1.0.0.110, R6250 before 1.0.4.34, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700 before 1.0.2.6, R6700v3 before 1.0.2.66, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7100LG before 1.0.0.50, R7300 before 1.0.0.70, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, R8500 before 1.0.2.128, WNDR3400v3 before 1.0.1.24, WNR3500Lv2 before 1.2.0.62, and XR500 before 2.3.2.56.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21933	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'esn_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-45668	Certain NETGEAR devices are affected by stored XSS. This affects EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, R7960P before 1.4.1.66, R7900P before 1.4.1.66, R8000P before 1.4.1.66, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX45 before 1.0.2.72, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	6.5	More Details
CVE-2021-31558	DIAEnergie Version 1.7.5 and prior is vulnerable to stored cross-site scripting when an unauthenticated user injects arbitrary code into the parameter "descr" of the script "DIAE_hierarchyHandler.ashx".	6.5	More Details
CVE-2021-36886	Cross-Site Request Forgery (CSRF) vulnerability discovered in Contact Form 7 Database Addon – CFDB7 WordPress plugin (versions <= 1.2.5.9).	6.5	More Details
CVE-2020-20595	A cross-site request forgery (CSRF) in OPMS v1.3 and below allows attackers to arbitrarily add a user account via /user/add.	6.5	More Details
CVE-2021-38009	Inappropriate implementation in cache in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-45498	NETGEAR R6700v2 devices before 1.2.0.88 are affected by authentication bypass.	6.5	More Details
CVE-2021-43156	In ProjectWorlds Online Book Store PHP 1.0 a CSRF vulnerability in admin_delete.php allows a remote attacker to delete any book.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45670	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, R7000 before 1.0.11.116, R7900 before 1.0.4.38, R8000 before 1.0.4.68, RAX200 before 1.0.3.106, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, EX3700 before 1.0.0.90, MR60 before 1.0.6.110, R7000P before 1.3.2.126, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, EX3800 before 1.0.0.90, MS60 before 1.0.6.110, R6900P before 1.3.2.126, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	6.5	More Details
CVE-2021-45667	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, R7960P before 1.4.1.66, RAX200 before 1.0.3.106, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, EX3700 before 1.0.0.90, MR60 before 1.0.6.110, R8000P before 1.4.1.66, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, EX3800 before 1.0.0.90, MS60 before 1.0.6.110, R7900P before 1.4.1.66, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	6.5	More Details
CVE-2021-21935	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ‘host_alt_filter2’ parameter. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-45666	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX80 before 1.0.1.64, EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, RBW30 before 2.6.1.4, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, and RBS40V before 2.6.1.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45665	Certain NETGEAR devices are affected by stored XSS. This affects EAX20 before 1.0.0.36, EAX80 before 1.0.1.62, EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, RBW30 before 2.6.1.4, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, and RBS40V before 2.6.1.4.	6.5	More Details
CVE-2021-45495	NETGEAR D7000 devices before 1.0.1.68 are affected by authentication bypass.	6.5	More Details
CVE-2021-41788	MediaTek microchips, as used in NETGEAR devices through 2021-12-13 and other devices, mishandle attempts at Wi-Fi authentication flooding. (Affected Chipsets MT7603E, MT7612, MT7613, MT7615, MT7622, MT7628, MT7629, MT7915; Affected Software Versions 7.4.0.0).	6.5	More Details
CVE-2021-45483	In WebKitGTK before 2.32.4, there is a use-after-free in WebCore::Frame::page, a different vulnerability than CVE-2021-30889.	6.5	More Details
CVE-2021-45482	In WebKitGTK before 2.32.4, there is a use-after-free in WebCore::ContainerNode::firstChild, a different vulnerability than CVE-2021-30889.	6.5	More Details
CVE-2021-45481	In WebKitGTK before 2.32.4, there is incorrect memory allocation in WebCore::ImageBufferCairoImageSurfaceBackend::create, leading to a segmentation violation and application crash, a different vulnerability than CVE-2021-30889.	6.5	More Details
CVE-2021-21937	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ‘host_alt_filter’ parameter. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-21934	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at ‘imei_filter’ parameter. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-38018	Inappropriate implementation in navigation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21932	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this at 'name_filter' parameter. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-21896	A directory traversal vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary file deletion. An attacker can make an authenticated HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2021-45519	NETGEAR XR1000 devices before 1.0.0.58 are affected by denial of service.	6.5	More Details
CVE-2021-45518	NETGEAR XR1000 devices before 1.0.0.58 are affected by denial of service.	6.5	More Details
CVE-2021-45517	NETGEAR XR1000 devices before 1.0.0.58 are affected by denial of service.	6.5	More Details
CVE-2021-21908	Specially-crafted command line arguments can lead to arbitrary file deletion. The handle_delete function does not attempt to sanitize or otherwise validate the contents of the [file] parameter (passed to the function as argv[1]), allowing an authenticated attacker to supply directory traversal primitives and delete semi-arbitrary files.	6.5	More Details
CVE-2021-43548	Patient Information Center iX (PIC iX) Versions C.02 and C.03 receives input or data, but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly.	6.5	More Details
CVE-2021-24997	The WP Guppy WordPress plugin before 1.3 does not have any authorisation in some of the REST API endpoints, allowing any user to call them and could lead to sensitive information disclosure, such as usernames and chats between users, as well as be able to send messages as an arbitrary user	6.5	More Details
CVE-2021-45515	Certain NETGEAR devices are affected by denial of service. This affects EX7500 before 1.0.0.72, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, RBRE960 before 6.0.3.68, RBSE960 before 6.0.3.68, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, and RBK852 before 3.2.17.12.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21922	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ‘username_filter’ parameter with the administrative account or through cross-site request forgery.	6.5	More Details
CVE-2021-21924	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at ‘desc_filter’ parameter.	6.5	More Details
CVE-2021-21925	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at ‘firm_filter’ parameter.	6.5	More Details
CVE-2021-21926	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at ‘health_filter’ parameter.	6.5	More Details
CVE-2021-21927	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger these vulnerabilities. This can be done as any authenticated user or through cross-site request forgery at ‘loc_filter’ parameter.	6.5	More Details
CVE-2021-21928	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at ‘mac_filter’ parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-21929	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at ‘prod_filter’ parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-21930	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at ‘sn_filter’ parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details
CVE-2021-21931	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests at‘ stat_filter’ parameter to trigger this vulnerability. This can be done as any authenticated user or through cross-site request forgery.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38010	Inappropriate implementation in service workers in Google Chrome prior to 96.0.4664.45 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2021-45671	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX80 before 1.0.1.62, EX7500 before 1.0.0.72, R7900 before 1.0.4.38, R8000 before 1.0.4.68, RAX200 before 1.0.4.120, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, MR60 before 1.0.6.110, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.4.120, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.4.120, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	6.5	More Details
CVE-2021-4059	Insufficient data validation in loader in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-4068	Insufficient data validation in new tab page in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-45647	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects EAX80 before 1.0.1.62, EX7000 before 1.0.1.104, R6120 before 1.0.0.76, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.78, R6850 before 1.1.0.78, R6350 before 1.1.0.78, R6330 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R7000 before 1.0.11.116, R6900P before 1.3.3.140, R7000P before 1.3.3.140, R7200 before 1.2.0.76, R7350 before 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, R7900 before 1.0.4.38, R7960P before 1.4.1.66, R8000 before 1.0.4.68, R7900P before 1.4.1.66, R8000P before 1.4.1.66, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX45 before 1.0.2.72, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	6.5	More Details
CVE-2021-38019	Insufficient policy enforcement in CORS in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45608	Certain D-Link, Edimax, NETGEAR, TP-Link, Tenda, and Western Digital devices are affected by an integer overflow by an unauthenticated attacker. Remote code execution from the WAN interface (TCP port 20005) cannot be ruled out; however, exploitability was judged to be of "rather significant complexity" but not "impossible." The overflow is in SoftwareBus_dispatchNormalEPMsgOut in the KCodes NetUSB kernel module. Affected NETGEAR devices are D7800 before 1.0.1.68, R6400v2 before 1.0.4.122, and R6700v3 before 1.0.4.122.	6.5	More Details
CVE-2021-4024	A flaw was found in podman. The `podman machine` function (used to create and manage Podman virtual machine containing a Podman process) spawns a `gvproxy` process on the host system. The `gvproxy` API is accessible on port 7777 on all IP addresses on the host. If that port is open on the host's firewall, an attacker can potentially use the `gvproxy` API to forward ports on the host to ports in the VM, making private services on the VM accessible to the network. This issue could be also used to interrupt the host's services by forwarding all ports to the VM.	6.5	More Details
CVE-2021-4054	Incorrect security UI in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	6.5	More Details
CVE-2021-38021	Inappropriate implementation in referrer in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2021-39013	IBM Cloud Pak for Security (CP4S) 1.7.2.0, 1.7.1.0, and 1.7.0.0 could allow an authenticated user to obtain sensitive information in HTTP responses that could be used in further attacks against the system. IBM X-Force ID: 213651.	6.5	More Details
CVE-2021-38022	Inappropriate implementation in WebAuthentication in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-40579	https://www.sourcecodester.com/ Online Enrollment Management System in PHP and PayPal Free Source Code 1.0 is affected by: Incorrect Access Control. The impact is: gain privileges (remote).	6.5	More Details
CVE-2021-35032	A vulnerability in the 'libsal.so' of the Zyxel GS1900 series firmware version 2.60 could allow an authenticated local user to execute arbitrary OS commands via a crafted function call.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45552	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.48, R7800 before 1.0.2.68, R8900 before 1.0.5.2, R9000 before 1.0.5.2, RAX120 before 1.0.1.108, and XR700 before 1.0.1.20.	6.3	More Details
CVE-2021-45548	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.60, DM200 before 1.0.0.66, EX2700 before 1.0.1.56, EX6150v2 before 1.0.1.86, EX6200v2 before 1.0.1.86, EX6250 before 1.0.0.128, EX6400 before 1.0.2.144, EX6400v2 before 1.0.0.128, EX6410 before 1.0.0.128, EX6420 before 1.0.0.128, EX7300 before 1.0.2.144, EX7300v2 before 1.0.0.128, EX7320 before 1.0.0.128, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.26, R9000 before 1.0.5.2, RAX120 before 1.0.1.128, WN3000RPv2 before 1.0.0.78, WN3000RPv3 before 1.0.2.80, WNR2000v5 before 1.0.0.74, XR500 before 2.3.2.66, RBK20 before 2.7.3.22, RBR20 before 2.7.3.22, RBS20 before 2.7.3.22, RBK40 before 2.7.3.22, RBR40 before 2.7.3.22, and RBS40 before 2.7.3.22.	6.3	More Details
CVE-2021-43849	cordova-plugin-fingerprint-aio is a plugin provides a single and simple interface for accessing fingerprint APIs on both Android 6+ and iOS. In versions prior to 5.0.1 The exported activity `de.niklasmerz.cordova.biometric.BiometricActivity` can cause the app to crash. This vulnerability occurred because the activity didn't handle the case where it is requested with invalid or empty data which results in a crash. Any third party app can constantly call this activity with no permission. A 3rd party app/attacker using event listener can continually stop the app from working and make the victim unable to open it. Version 5.0.1 of the cordova-plugin-fingerprint-aio doesn't export the activity anymore and is no longer vulnerable. If you want to fix older versions change the attribute android:exported in plugin.xml to false. Please upgrade to version 5.0.1 as soon as possible.	6.2	More Details
CVE-2021-45472	In MediaWiki through 1.37, XSS can occur in Wikibase because an external identifier property can have a URL format that includes a $1 formatter substitution marker, and the javascript: URL scheme (among others) can be used.	6.1	More Details
CVE-2021-45522	NETGEAR XR1000 devices before 1.0.0.58 are affected by a hardcoded password.	6.1	More Details
CVE-2020-20425	S-CMS Government Station Building System v5.0 contains a cross-site scripting (XSS) vulnerability in the search function.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45425	Reflected Cross Site Scripting (XSS) in SAFARI Montage versions 8.3 and 8.5 allows remote attackers to execute JavaScript codes.	6.1	More Details
CVE-2021-36885	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability discovered in Contact Form 7 Database Addon – CFDB7 WordPress plugin (versions <= 1.2.6.1).	6.1	More Details
CVE-2021-45603	Certain NETGEAR devices are affected by disclosure of sensitive information. A UPnP request reveals a device's serial number, which can be used for a password reset. This affects D7800 before 1.0.1.66, EX2700 before 1.0.1.68, WN3000RPv2 before 1.0.0.90, WN3000RPv3 before 1.0.2.100, LBR1020 before 2.6.5.20, LBR20 before 2.6.5.32, R6700AX before 1.0.10.110, R7800 before 1.0.2.86, R8900 before 1.0.5.38, R9000 before 1.0.5.38, RAX10 before 1.0.10.110, RAX120v1 before 1.2.3.28, RAX120v2 before 1.2.3.28, RAX70 before 1.0.10.110, RAX78 before 1.0.10.110, XR450 before 2.3.2.130, XR500 before 2.3.2.130, and XR700 before 1.0.1.46.	6.1	More Details
CVE-2021-45602	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.66, EX2700 before 1.0.1.68, WN3000RPv2 before 1.0.0.90, WN3000RPv3 before 1.0.2.100, LBR1020 before 2.6.5.20, LBR20 before 2.6.5.32, R6700AX before 1.0.10.110, R7800 before 1.0.2.86, R8900 before 1.0.5.38, R9000 before 1.0.5.38, RAX10 before 1.0.10.110, RAX120v1 before 1.2.3.28, RAX120v2 before 1.2.3.28, RAX70 before 1.0.10.110, RAX78 before 1.0.10.110, XR450 before 2.3.2.130, XR500 before 2.3.2.130, and XR700 before 1.0.1.46.	6.1	More Details
CVE-2021-44030	Quest KACE Desktop Authority before 11.2 allows XSS because it does not prevent untrusted HTML from reaching the jQuery.htmlPrefilter method of jQuery.	6.1	More Details
CVE-2021-24967	The Contact Form & Lead Form Elementor Builder WordPress plugin before 1.6.4 does not sanitise and escape some lead values, which could allow unauthenticated users to perform Cross-Site Scripting attacks against logged in admin viewing the inserted Leads	6.1	More Details
CVE-2020-20597	A cross-site scripting (XSS) vulnerability in the potrtalItemName parameter in \web\PortalController.java of lemon V1.10.0 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24797	The Tickera WordPress plugin before 3.4.8.3 does not properly sanitise and escape the Name fields of booked Events before outputting them in the Orders admin dashboard, which could allow unauthenticated users to perform Cross-Site Scripting attacks against admins.	6.1	More Details
CVE-2021-45903	A persistent cross-site scripting (XSS) issue in the web interface of SuiteCRM before 7.10.35, and 7.11.x and 7.12.x before 7.12.2, allows a remote attacker to introduce arbitrary JavaScript via attachments upload, a different vulnerability than CVE-2021-39267 and CVE-2021-39268.	6.1	More Details
CVE-2021-20875	Open redirect vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows a remote unauthenticated attacker to redirect users to arbitrary web sites and conduct phishing attacks by having a user to access a specially crafted URL.	6.1	More Details
CVE-2021-45473	In MediaWiki through 1.37, Wikibase item descriptions allow XSS, which is triggered upon a visit to an action=info URL (aka a page-information sidebar).	6.1	More Details
CVE-2021-45895	Netgen Tags Bundle 3.4.x before 3.4.11 and 4.0.x before 4.0.15 allows XSS in the Tags Admin interface.	6.1	More Details
CVE-2020-20426	S-CMS Government Station Building System v5.0 contains a cross-site scripting (XSS) vulnerability in /function/booksave.php.	6.1	More Details
CVE-2020-20598	A cross-site scripting (XSS) vulnerability in the Editing component of lemon V1.10.0 allows attackers to execute arbitrary web scripts or HTML.	6.1	More Details
CVE-2021-45663	NETGEAR R7000 devices before 1.0.11.126 are affected by stored XSS.	6.1	More Details
CVE-2021-24984	The WPFront User Role Editor WordPress plugin before 3.2.1.11184 does not sanitise and escape the changes-saved parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-45662	NETGEAR R7000 devices before 1.0.9.88 are affected by stored XSS.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45525	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects EX7000 before 1.0.1.80, R6400 before 1.0.1.50, R6400v2 before 1.0.4.118, R6700 before 1.0.2.8, R6700v3 before 1.0.4.118, R6900 before 1.0.2.8, R6900P before 1.3.2.124, R7000 before 1.0.9.88, R7000P before 1.3.2.124, R7900 before 1.0.3.18, R7900P before 1.4.1.50, R8000 before 1.0.4.46, R8000P before 1.4.1.50, RAX80 before 1.0.1.56, and WNR3500Lv2 before 1.2.0.62.	6.1	More Details
CVE-2021-44543	An XSS vulnerability was found in Privoxy which was fixed in cgi_error_no_template() by encode the template name when Privoxy is configured to servce the user-manual itself.	6.1	More Details
CVE-2021-45813	SLICAN WebCTI 1.01 2015 is affected by a Cross Site Scripting (XSS) vulnerability. The attacker can steal the user's session by injecting malicious JavaScript codes which leads to Session Hijacking and cause user's credentials theft.	6.1	More Details
CVE-2021-43552	The use of a hard-coded cryptographic key significantly increases the possibility encrypted data may be recovered from the Patient Information Center iX (PIC iX) Versions B.02, C.02, and C.03.	6.1	More Details
CVE-2021-38961	IBM OPENBMC OP910 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 212049.	6.1	More Details
CVE-2021-45812	NUUO Network Video Recorder NVRsolo 3.9.1 is affected by a Cross Site Scripting (XSS) vulnerability. An attacker can steal the user's session by injecting malicious JavaScript codes which leads to session hijacking.	6.1	More Details
CVE-2021-45474	In MediaWiki through 1.37, the Special:ImportFile URI (aka FileImporter) allows XSS, as demonstrated by the clientUrl parameter.	6.1	More Details
CVE-2021-24980	The Gwolle Guestbook WordPress plugin before 4.2.0 does not sanitise and escape the gwolle_gb_user_email parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue in an admin page	6.1	More Details
CVE-2020-20605	Blog CMS v1.0 contains a cross-site scripting (XSS) vulnerability in the /controller/CommentAdminController.java component.	6.1	More Details
CVE-2021-4169	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24979	The Paid Memberships Pro WordPress plugin before 2.6.6 does not escape the s parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-44598	Attendance Management System 1.0 is affected by a Cross Site Scripting (XSS) vulnerability. The value of the FirstRecord request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The attacker can access the system, by using the XSS-reflected method, and then can store information by injecting the admin account on this system.	6.1	More Details
CVE-2021-45605	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400 before 1.0.1.68, R7000 before 1.0.11.116, R6900P before 1.3.3.140, R7000P before 1.3.3.140, R7900 before 1.0.4.38, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, and XR300 before 1.0.3.50.	6.0	More Details
CVE-2021-43550	The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive information, which affects the communications between Patient Information Center iX (PIC iX) Versions C.02 and C.03 and Efficia CM Series Revisions A.01 to C.0x and 4.0.	5.9	More Details
CVE-2021-45675	Certain NETGEAR devices are affected by stored XSS. This affects R6120 before 1.0.0.76, R6260 before 1.1.0.78, R6850 before 1.1.0.78, R6350 before 1.1.0.78, R6330 before 1.1.0.78, R6800 before 1.2.0.76, R6700v2 before 1.2.0.76, R6900v2 before 1.2.0.76, R7200 before 1.2.0.76, R7350 before 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, and AC2600 before 1.2.0.76.	5.8	More Details
CVE-2021-45523	NETGEAR R7000 devices before 1.0.9.42 are affected by a buffer overflow by an authenticated user.	5.7	More Details
CVE-2021-45664	NETGEAR R7000 devices before 1.0.11.126 are affected by stored XSS.	5.6	More Details
CVE-2019-8702	This issue was addressed with a new entitlement. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra, iOS 12.4, tvOS 12.4. A local user may be able to read a persistent account identifier.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45256	A Null Pointer Dereference vulnerability existfs in nasm 2.16rc0 via asm/preproc.c.	5.5	More Details
CVE-2021-45258	A stack overflow vulnerability exists in gpac 1.1.0 via the gf_bifs_dec_proto_list function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-45263	An invalid free vulnerability exists in gpac 1.1.0 via the gf_svg_delete_attribute_value function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-44028	XXE can occur in Quest KACE Desktop Authority before 11.2 because the log4net configuration file might be controlled by an attacker, a related issue to CVE-2018-1285.	5.5	More Details
CVE-2021-45480	An issue was discovered in the Linux kernel before 5.15.11. There is a memory leak in the __rds_conn_create() function in net/rds/connection.c in a certain combination of circumstances.	5.5	More Details
CVE-2021-45259	An Invalid pointer reference vulnerability exists in gpac 1.1.0 via the gf_svg_node_del function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2021-30767	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.6.2, macOS Monterey 12.1, Security Update 2021-008 Catalina, iOS 15.2 and iPadOS 15.2, watchOS 8.3. A local user may be able to modify protected parts of the file system.	5.5	More Details
CVE-2021-45267	An invalid memory address dereference vulnerability exists in gpac 1.1.0 via the svg_node_start function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2017-13910	An access issue was addressed with additional sandbox restrictions on applications. This issue is fixed in macOS High Sierra 10.13. An application may be able to access restricted files.	5.5	More Details
CVE-2021-45257	An infinite loop vulnerability exists in nasm 2.16rc0 via the gpaste_tokens function.	5.5	More Details
CVE-2021-45262	An invalid free vulnerability exists in gpac 1.1.0 via the gf_sg_command_del function, which causes a segmentation fault and application crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3896	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra. A malicious application may be able to overwrite arbitrary files.	5.5	More Details
CVE-2021-45261	An Invalid Pointer vulnerability exists in GNU patch 2.7 via the another_hunk function, which causes a Denial of Service.	5.5	More Details
CVE-2021-45260	A null pointer dereference vulnerability exists in gpac 1.1.0 in the lsr_read_id.part function, which causes a segmentation fault and application crash.	5.5	More Details
CVE-2017-13909	An issue existed in the storage of sensitive tokens. This issue was addressed by placing the tokens in Keychain. This issue is fixed in macOS High Sierra 10.13. A local attacker may gain access to iCloud authentication tokens.	5.5	More Details
CVE-2021-4179	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2020-20946	Qibosoft v7 contains a stored cross-site scripting (XSS) vulnerability in the component /admin/index.php?lfj=friendlink&action=add.	5.4	More Details
CVE-2021-4072	elgg is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-3977	invoiceninja is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-24988	The WP RSS Aggregator WordPress plugin before 4.19.3 does not sanitise and escape data before outputting it in the System Info admin dashboard, which could lead to a Stored XSS issue due to the wprss_dismiss_addon_notice AJAX action missing authorisation and CSRF checks, allowing any authenticated users, such as subscriber to call it and set a malicious payload in the addon parameter.	5.4	More Details
CVE-2021-45636	NETGEAR D7000 devices before 1.0.1.82 are affected by a stack-based buffer overflow by an unauthenticated attacker.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45906	OpenWrt 21.02.1 allows XSS via the NAT Rules Name screen.	5.4	More Details
CVE-2021-24969	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks	5.4	More Details
CVE-2021-45905	OpenWrt 21.02.1 allows XSS via the Traffic Rules Name screen.	5.4	More Details
CVE-2020-20600	MetInfo 7.0 beta contains a stored cross-site scripting (XSS) vulnerability in the $name parameter of admin/?n=column&c=index&a=doAddColumn.	5.4	More Details
CVE-2021-45904	OpenWrt 21.02.1 allows XSS via the Port Forwards Add Name screen.	5.4	More Details
CVE-2021-4177	livehelperchat is vulnerable to Generation of Error Message Containing Sensitive Information	5.3	More Details
CVE-2021-45471	In MediaWiki through 1.37, blocked IP addresses are allowed to edit EntitySchema items.	5.3	More Details
CVE-2020-35398	An issue was discovered in UTI Mutual fund Android application 5.4.18 and prior, allows attackers to brute force enumeration of usernames determined by the error message returned after invalid credentials are attempted.	5.3	More Details
CVE-2021-35243	The HTTP PUT and DELETE methods were enabled in the Web Help Desk web server (12.7.7 and earlier), allowing users to execute dangerous HTTP requests. The HTTP PUT method is normally used to upload data that is saved on the server with a user-supplied URL. While the DELETE method requests that the origin server removes the association between the target resource and its current functionality. Improper use of these methods may lead to a loss of integrity.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45646	NETGEAR R7000 devices before 1.0.11.116 are affected by disclosure of sensitive information.	5.3	More Details
CVE-2021-45639	Certain NETGEAR devices are affected by reflected XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.32, EAX80 before 1.0.1.62, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7000 before 1.0.1.104, EX7500 before 1.0.0.72, R7000 before 1.0.11.110, R7900 before 1.0.4.30, R7960P before 1.4.1.66, R8000 before 1.0.4.62, RAX200 before 1.0.2.102, XR300 before 1.0.3.50, EX3700 before 1.0.0.90, MR60 before 1.0.5.102, R7000P before 1.3.2.126, R8000P before 1.4.1.66, RAX20 before 1.0.1.64, RAX50 before 1.0.2.28, RAX80 before 1.0.3.102, EX3800 before 1.0.0.90, MS60 before 1.0.5.102, R6900P before 1.3.2.126, R7900P before 1.4.1.66, RAX15 before 1.0.1.64, RAX45 before 1.0.2.28, RAX75 before 1.0.3.102, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	5.2	More Details
CVE-2021-45677	Certain NETGEAR devices are affected by stored XSS. This affects GS108Tv2 before 5.4.2.36 and GS110TPv2 before 5.4.2.36.	5.2	More Details
CVE-2021-21920	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ‘surname_filter’ parameter with the administrative account or through cross-site request forgery.	4.9	More Details
CVE-2021-21923	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ‘company_filter’ parameter with the administrative account or through cross-site request forgery.	4.9	More Details
CVE-2021-21921	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ‘name_filter’ parameter with the administrative account or through cross-site request forgery.	4.9	More Details
CVE-2021-21878	A local file inclusion vulnerability exists in the Web Manager Applications and FsBrowse functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted series of HTTP requests can lead to local file inclusion. An attacker can make a series of authenticated HTTP requests to trigger this vulnerability.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21919	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at ord' parameter. However, the high privilege super-administrator account needs to be used to achieve exploitation without cross-site request forgery attack.	4.9	More Details
CVE-2021-21918	A specially-crafted HTTP request can lead to SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability at 'name_filter' parameter. However, the high privilege super-administrator account needs to be used to achieve exploitation without cross-site request forgery attack.	4.9	More Details
CVE-2021-21907	A directory traversal vulnerability exists in the CMA CLI getenv command functionality of Garrett Metal Detectors' iC Module CMA Version 5.0. A specially-crafted command line argument can lead to local file inclusion. An attacker can provide malicious input to trigger this vulnerability.	4.9	More Details
CVE-2021-24902	The Typebot I Build beautiful conversational forms WordPress plugin before 1.4.3 does not sanitise and escape the Publish ID setting, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24992	The Smart Floating / Sticky Buttons WordPress plugin before 2.5.5 does not sanitise and escape some parameter before outputting them in attributes and page, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-45673	Certain NETGEAR devices are affected by stored XSS. This affects R7000 before 1.0.11.110, R7900 before 1.0.4.30, R8000 before 1.0.4.62, RAX200 before 1.0.3.106, R7000P before 1.3.3.140, RAX80 before 1.0.3.106, R6900P before 1.3.3.140, and RAX75 before 1.0.3.106.	4.8	More Details
CVE-2021-40836	A vulnerability affecting F-Secure antivirus engine was discovered whereby scanning MS outlook .pst files can lead to denial-of-service. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45641	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.72, D6000 before 1.0.0.72, D6200 before 1.1.00.34, D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7000 before 1.0.1.74, D7000v2 before 1.0.0.53, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DC112A before 1.0.0.42, DGN2200Bv4 before 1.0.0.109, DGN2200v4 before 1.0.0.110, DM200 before 1.0.0.61, EX3700 before 1.0.0.76, EX3800 before 1.0.0.76, EX6120 before 1.0.0.46, EX6130 before 1.0.0.28, EX7000 before 1.0.1.78, PR2000 before 1.0.0.28, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6250 before 1.0.4.34, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700v3 before 1.0.2.66, R6700 before 1.0.2.6, R6900 before 1.0.2.6, R7000 before 1.0.9.34, R7100LG before 1.0.0.50, R7500v2 before 1.0.3.40, R7900P before 1.4.1.50, R8000P before 1.4.1.50, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBR40 before 2.3.0.28, RBS40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, WN3000RPv2 before 1.0.0.78, WNDR3400v3 before 1.0.1.24, WNR2000v5 before 1.0.0.70, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.56.	4.6	More Details
CVE-2021-45530	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R7000 before 1.0.11.126, R7960P before 1.4.2.84, R8000 before 1.0.4.74, RAX200 before 1.0.4.120, R8000P before 1.4.2.84, RAX20 before 1.0.2.82, RAX45 before 1.0.2.82, RAX80 before 1.0.4.120, R7900P before 1.4.2.84, RAX15 before 1.0.2.82, RAX50 before 1.0.2.82, and RAX75 before 1.0.4.120.	4.5	More Details
CVE-2021-45604	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects CBR750 before 3.2.18.2, D6220 before 1.0.0.68, D6400 before 1.0.0.102, D8500 before 1.0.3.60, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6300v2 before 1.0.4.50, R6400 before 1.0.1.68, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.116, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.38, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, and XR1000 before 1.0.0.58.	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45606	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400 before 1.0.1.70, R7000 before 1.0.11.126, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RS400 before 1.5.1.80, R6400v2 before 1.0.4.118, R7000P before 1.3.3.140, RAX80 before 1.0.4.120, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, and RAX75 before 1.0.4.120.	4.5	More Details
CVE-2021-27006	StorageGRID (formerly StorageGRID Webscale) versions 11.5 prior to 11.5.0.5 are susceptible to a vulnerability which may allow an administrative user to escalate their privileges and modify settings in SANtricity System Manager.	4.4	More Details
CVE-2021-3622	A flaw was found in the hivex library. This flaw allows an attacker to input a specially crafted Windows Registry (hive) file, which would cause hivex to recursively call the _get_children() function, leading to a stack overflow. The highest threat from this vulnerability is to system availability.	4.3	More Details
CVE-2021-38020	Insufficient policy enforcement in contacts picker in Google Chrome on Android prior to 96.0.4664.45 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2021-45676	Certain NETGEAR devices are affected by stored XSS. This affects RAX200 before 1.0.5.126, RAX20 before 1.0.2.82, RAX80 before 1.0.5.126, RAX15 before 1.0.2.82, and RAX75 before 1.0.5.126.	4.3	More Details
CVE-2020-20943	A Cross-Site Request Forgery (CSRF) in /member/post.php?job=postnew&step=post of Qibosoft v7 allows attackers to force victim users into arbitrarily publishing new articles via a crafted URL.	4.3	More Details
CVE-2021-43158	In ProjectWorlds Online Shopping System PHP 1.0, a CSRF vulnerability in cart_remove.php allows a remote attacker to remove any product in the customer's cart.	4.3	More Details
CVE-2021-4162	archivy is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-21886	A directory traversal vulnerability exists in the Web Manager FSBrowsePage functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially crafted HTTP request can lead to information disclosure. An attacker can make an authenticated HTTP request to trigger this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45672	Certain NETGEAR devices are affected by Stored XSS. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6120 before 1.0.0.76, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R6850 before 1.1.0.78, R7200 before 1.2.0.76, R7350 before 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, and RAX40 before 1.0.3.62.	4.2	More Details
CVE-2021-45653	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	3.9	More Details
CVE-2021-45640	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.72, D6000 before 1.0.0.72, D6200 before 1.1.00.34, D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7000 before 1.0.1.74, D7000v2 before 1.0.0.53, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DC112A before 1.0.0.42, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.109, DM200 before 1.0.0.61, EX3700 before 1.0.0.76, EX3800 before 1.0.0.76, EX6120 before 1.0.0.46, EX6130 before 1.0.0.28, EX7000 before 1.0.1.78, PR2000 before 1.0.0.28, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6250 before 1.0.4.34, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700 before 1.0.2.6, R6700v3 before 1.0.2.66, R6900 before 1.0.2.6, R7000 before 1.0.9.34, R7100LG before 1.0.0.50, R7500v2 before 1.0.3.40, R7900P before 1.4.1.50, R8000P before 1.4.1.50, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.28, RBK40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR20 before 2.3.0.28, RBR40 before 2.3.0.28, RBR50 before 2.3.0.32, RBS20 before 2.3.0.28, RBS40 before 2.3.0.28, RBS50 before 2.3.0.32, WN3000RPv2 before 1.0.0.78, WNDR3400v3 before 1.0.1.24, WNR2000v5 before 1.0.0.70, WNR2020 before 1.1.0.62, WNR3500Lv2 before 1.2.0.62, XR450 before 2.3.2.56, and XR500 before 2.3.2.56.	3.9	More Details
CVE-2021-45669	Certain NETGEAR devices are affected by stored XSS. This affects RAX200 before 1.0.3.106, MR60 before 1.0.6.110, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	3.7	More Details
CVE-2021-45486	In the IPv4 implementation in the Linux kernel before 5.12.4, net/ipv4/route.c has an information leak because the hash table is very small.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-2375	An issue existed in preventing the uploading of CallKit call history to iCloud. This issue was addressed through improved logic. This issue is fixed in iOS 10.2.1. Updates for CallKit call history are sent to iCloud.	3.3	More Details
CVE-2021-45674	Certain NETGEAR devices are affected by stored XSS. This affects R7000 before 1.0.11.110, R7900 before 1.0.4.30, R8000 before 1.0.4.62, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	3.2	More Details
CVE-2021-45648	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects EX6100v2 before 1.0.1.106, EX6150v2 before 1.0.1.106, EX6250 before 1.0.0.146, EX6400 before 1.0.2.164, EX6400v2 before 1.0.0.146, EX6410 before 1.0.0.146, EX6420 before 1.0.0.146, EX7300 before 1.0.2.164, EX7300v2 before 1.0.0.146, EX7320 before 1.0.0.146, EX7700 before 1.0.0.222, LBR1020 before 2.6.5.16, LBR20 before 2.6.5.2, RBK352 before 4.3.4.7, RBK50 before 2.7.3.22, RBR350 before 4.3.4.7, RBR50 before 2.7.3.22, and RBS350 before 4.3.4.7.	3.1	More Details
CVE-2021-23151	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
CVE-2021-3090	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-43553. Reason: This candidate is a reservation duplicate of CVE-2021-43553. Notes: All CVE users should reference CVE-2021-43553 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-3095	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-43551. Reason: This candidate is a reservation duplicate of CVE-2021-43551. Notes: All CVE users should reference CVE-2021-43551 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2016-3736	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2016. Notes: non	N/A	More Details
CVE-2021-3892	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-18198. Reason: This candidate is a reservation duplicate of CVE-2019-18198. Notes: All CVE users should reference CVE-2019-18198 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4114	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-44771	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
CVE-2021-4113	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2016-3103	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2016. Notes: non	N/A	More Details