Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
3DS					
teamwork_cloud					
Incorrect Permission Assignment for Critical Resource	28-Dec-20	7.2	An incorrect permission assignment (chmod 777) of /etc/environment during the installation script of No Magic TeamworkCloud 18.0 through 19.0 allows any local unprivileged user to write to /etc/environment. An attacker can escalate to root by writing arbitrary code to this file, which would be executed by root during the next login, reboot, or sourcing of the environment. **CVE ID : CVE-2020-25507**	N/A	A-3DS-TEAM-040121/1
ABB					
symphony_plus_historian					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-20	7.5	In S+ Operations and S+ Historian, a successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on	N/A	A-ABB-SYMP-040121/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the DBMS file system and in some cases issue commands to the operating system. This can lead to a loss of confidentiality and data integrity or even affect the product behavior and its availability. **CVE ID : CVE-2020-24673**		
Incorrect Authorization	22-Dec-20	9	In S+ Operations and S+ Historian, not all client commands correctly check user permission as expected. Authenticated but Unauthorized remote users could execute a Denial-of-Service (DoS) attack, execute arbitrary code, or obtain more privilege than intended on the machines. **CVE ID : CVE-2020-24674**	N/A	A-ABB-SYMP-040121/3
Improper Authentication	22-Dec-20	7.5	In S+ Operations and S+ History, it is possible that an unauthenticated user could inject values to the Operations History server (or standalone S+ History server) and ultimately write values to the controlled process. **CVE ID : CVE-2020-24675**	N/A	A-ABB-SYMP-040121/4
Improper Check for Unusual or Exceptional Conditions	22-Dec-20	6.5	Vulnerabilities in the S+ Operations and S+ Historian web applications can lead to a possible code execution and privilege escalation, redirect the user somewhere else or	N/A	A-ABB-SYMP-040121/5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			download unwanted data. **CVE ID : CVE-2020-24677**		
Improper Privilege Management	22-Dec-20	6.5	An authenticated user might execute malicious code under the user context and take control of the system. S+ Operations or S+ Historian database is affected by multiple vulnerabilities such as the possibility to allow remote authenticated users to gain high privileges. **CVE ID : CVE-2020-24678**	N/A	A-ABB-SYMP-040121/6
Improper Input Validation	22-Dec-20	10	A S+ Operations and S+ Historian service is subject to a DoS by special crafted messages. An attacker might use this flaw to make it crash or even execute arbitrary code on the machine where the service is hosted. **CVE ID : CVE-2020-24679**	N/A	A-ABB-SYMP-040121/7
Insufficiently Protected Credentials	22-Dec-20	4.6	In S+ Operations and S+ Historian, the passwords of internal users (not Windows Users) are encrypted but improperly stored in a database. **CVE ID : CVE-2020-24680**	N/A	A-ABB-SYMP-040121/8
Incorrect Resource Transfer Between Spheres	22-Dec-20	7.5	The affected versions of S+ Operations (version 2.1 SP1 and earlier) used an approach for user authentication which relies on validation at the client node (client-side authentication). This is not	N/A	A-ABB-SYMP-040121/9

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as secure as having the server validate a client application before allowing a connection. Therefore, if the network communication or endpoints for these applications are not protected, unauthorized actors can bypass authentication and make unauthorized connections to the server application. **CVE ID : CVE-2020-24683**		
symphony_plus_operations					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-20	7.5	In S+ Operations and S+ Historian, a successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. This can lead to a loss of confidentiality and data integrity or even affect the product behavior and its availability. **CVE ID : CVE-2020-24673**	N/A	A-ABB-SYMP-040121/10
Incorrect Authorization	22-Dec-20	9	In S+ Operations and S+ Historian, not all client commands correctly check	N/A	A-ABB-SYMP-040121/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user permission as expected. Authenticated but Unauthorized remote users could execute a Denial-of-Service (DoS) attack, execute arbitrary code, or obtain more privilege than intended on the machines. **CVE ID : CVE-2020-24674**		
Improper Authentication	22-Dec-20	7.5	In S+ Operations and S+ History, it is possible that an unauthenticated user could inject values to the Operations History server (or standalone S+ History server) and ultimately write values to the controlled process. **CVE ID : CVE-2020-24675**	N/A	A-ABB-SYMP-040121/12
Improper Check for Unusual or Exceptional Conditions	22-Dec-20	6.5	Vulnerabilities in the S+ Operations and S+ Historian web applications can lead to a possible code execution and privilege escalation, redirect the user somewhere else or download unwanted data. **CVE ID : CVE-2020-24677**	N/A	A-ABB-SYMP-040121/13
Improper Privilege Management	22-Dec-20	6.5	An authenticated user might execute malicious code under the user context and take control of the system. S+ Operations or S+ Historian database is affected by multiple vulnerabilities such as the possibility to allow remote authenticated users to gain	N/A	A-ABB-SYMP-040121/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			high privileges. **CVE ID : CVE-2020-24678**		
Improper Input Validation	22-Dec-20	10	A S+ Operations and S+ Historian service is subject to a DoS by special crafted messages. An attacker might use this flaw to make it crash or even execute arbitrary code on the machine where the service is hosted. **CVE ID : CVE-2020-24679**	N/A	A-ABB-SYMP-040121/15
Insufficiently Protected Credentials	22-Dec-20	4.6	In S+ Operations and S+ Historian, the passwords of internal users (not Windows Users) are encrypted but improperly stored in a database. **CVE ID : CVE-2020-24680**	N/A	A-ABB-SYMP-040121/16
Incorrect Resource Transfer Between Spheres	22-Dec-20	7.5	The affected versions of S+ Operations (version 2.1 SP1 and earlier) used an approach for user authentication which relies on validation at the client node (client-side authentication). This is not as secure as having the server validate a client application before allowing a connection. Therefore, if the network communication or endpoints for these applications are not protected, unauthorized actors can bypass authentication and make unauthorized connections	N/A	A-ABB-SYMP-040121/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server application. **CVE ID : CVE-2020-24683**		
symphony_\+_historian					
Improper Privilege Management	22-Dec-20	4.6	In Symphony Plus Operations and Symphony Plus Historian, some services can be vulnerable to privilege escalation attacks. An unprivileged (but authenticated) user could execute arbitrary code and result in privilege escalation, depending on the user that the service runs as. **CVE ID : CVE-2020-24676**	N/A	A-ABB-SYMP-040121/18
symphony_\+_operations					
Improper Privilege Management	22-Dec-20	4.6	In Symphony Plus Operations and Symphony Plus Historian, some services can be vulnerable to privilege escalation attacks. An unprivileged (but authenticated) user could execute arbitrary code and result in privilege escalation, depending on the user that the service runs as. **CVE ID : CVE-2020-24676**	N/A	A-ABB-SYMP-040121/19
advanced_comment_system_project					
advanced_comment_system					
Improper Limitation of a Pathname to a Restricted Directory ('Path	23-Dec-20	5	ACS Advanced Comment System 1.0 is affected by Directory Traversal via an advanced_component_system/index.php?ACS_path=..%2f URI.	N/A	A-ADV-ADVA-040121/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			**CVE ID : CVE-2020-35598**		
agentejo					
cockpit					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Dec-20	7.5	Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php check function. **CVE ID : CVE-2020-35846**	N/A	A-AGE-COCK-040121/21
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Dec-20	7.5	Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php resetpassword function. **CVE ID : CVE-2020-35847**	N/A	A-AGE-COCK-040121/22
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Dec-20	7.5	Agentejo Cockpit before 0.11.2 allows NoSQL injection via the Controller/Auth.php newpassword function. **CVE ID : CVE-2020-35848**	N/A	A-AGE-COCK-040121/23
alumni_management_system_project					
alumni_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Dec-20	7.5	SourceCodester Alumni Management System 1.0 is affected by SQL injection causing arbitrary remote code execution from GET input in view_event.php via the 'id' parameter. **CVE ID : CVE-2020-28070**	N/A	A-ALU-ALUM-040121/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-20	3.5	SourceCodester Alumni Management System 1.0 is affected by cross-site Scripting (XSS) in /admin/gallery.php. After the admin authentication an attacker can upload an image in the gallery using a XSS payload in the description textarea called 'about' and reach a stored XSS. **CVE ID : CVE-2020-28071**	N/A	A-ALU-ALUM-040121/25
Apache					
airflow					
Improper Privilege Management	21-Dec-20	3.5	Incorrect Session Validation in Apache Airflow Webserver versions prior to 1.10.14 with default config allows a malicious airflow user on site A where they log in normally, to access unauthorized Airflow Webserver on Site B through the session from Site A. This does not affect users who have changed the default value for `[webserver] secret_key` config. **CVE ID : CVE-2020-17526**	N/A	A-APA-AIRF-040121/26
pulsar_manager					
Incorrect Permission Assignment for Critical Resource	18-Dec-20	4	In the Pulsar manager 0.1.0 version, malicious users will be able to bypass pulsar-manager's admin, permission verification mechanism by constructing	N/A	A-APA-PULS-040121/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			special URLs, thereby accessing any HTTP API. **CVE ID : CVE-2020-17520**		
accumulo					
Incorrect Permission Assignment for Critical Resource	29-Dec-20	5.5	Apache Accumulo versions 1.5.0 through 1.10.0 and version 2.0.0 do not properly check the return value of some policy enforcement functions before permitting an authenticated user to perform certain administrative operations. Specifically, the return values of the 'canFlush' and 'canPerformSystemActions ' security functions are not checked in some instances, therefore allowing an authenticated user with insufficient permissions to perform the following actions: flushing a table, shutting down Accumulo or an individual tablet server, and setting or removing system-wide Accumulo configuration properties. **CVE ID : CVE-2020-17533**	N/A	A-APA-ACCU-040121/28
dolphinscheduler					
N/A	18-Dec-20	7.5	In DolphinScheduler 1.2.0 and 1.2.1, with mysql connectorj a remote code execution vulnerability exists when choosing mysql as database. **CVE ID : CVE-2020-11974**	N/A	A-APA-DOLP-040121/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tomee					
N/A	18-Dec-20	6.8	If Apache TomEE 8.0.0-M1 - 8.0.3, 7.1.0 - 7.1.3, 7.0.0-M1 - 7.0.8, 1.0.0 - 1.7.5 is configured to use the embedded ActiveMQ broker, and the broker config is misconfigured, a JMX port is opened on TCP port 1099, which does not include authentication. CVE-2020-11969 previously addressed the creation of the JMX management interface, however the incomplete fix did not cover this edge case. **CVE ID : CVE-2020-13931**	N/A	A-APA-TOME-040121/30
appbase					
streams					
Missing Authentication for Critical Function	16-Dec-20	10	The Appbase streams Docker image 2.1.2 contains a blank password for the root user. Systems deployed using affected versions of the streams container may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35468**	N/A	A-APP-STRE-040121/31
arc-swap_project					
arc-swap					
N/A	25-Dec-20	5	An issue has been discovered in the arc-swap crate before 0.4.8 (and 1.x before 1.1.0) for Rust. Use	N/A	A-ARC-ARC--040121/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of arc_swap::access::Map with the Constant test helper (or with a user-supplied implementation of the Access trait) could sometimes lead to dangling references being returned by the map. **CVE ID : CVE-2020-35711**		
ARM					
arm_compiler					
Out-of-bounds Write	24-Dec-20	4.4	Arm Compiler 5 through 5.06u6 has an error in a stack protection feature designed to help spot stack-based buffer overflows in local arrays. When this feature is enabled, a protected function writes a guard value to the stack prior to (above) any vulnerable arrays in the stack. The guard value is checked for corruption on function return; corruption leads to an error-handler call. In certain circumstances, the reference value that is compared against the guard value is itself also written to the stack (after any vulnerable arrays). The reference value is written to the stack when the function runs out of registers to use for other temporary data. If both the reference value and the guard value are written to	https://developer.arm.com/support/arm-security-updates/arm-compiler-5-stack-protection	A-ARM-ARM_-040121/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the stack, then the stack protection will fail to spot corruption when both values are overwritten with the same value. For both the reference value and the guard value to be corrupted, there would need to be both a buffer overflow and a buffer underflow in the vulnerable arrays (or some other vulnerability that causes two separated stack entries to be corrupted). **CVE ID : CVE-2020-24658**		
Atlassian					
crucible					
Unrestricted Upload of File with Dangerous Type	21-Dec-20	4	Affected versions of Atlassian Crucible allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the file upload request feature of code reviews. The affected versions are before version 4.7.4, and from version 4.8.0 before 4.8.5. **CVE ID : CVE-2020-29447**	N/A	A-ATL-CRUC-040121/34
backblaze					
backblaze					
Improper Certificate Validation	27-Dec-20	9.3	Backblaze for Windows before 7.0.1.433 and Backblaze for macOS before 7.0.1.434 suffer from improper certificate	N/A	A-BAC-BACK-040121/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation in `bztransmit` helper due to hardcoded whitelist of strings in URLs where validation is disabled leading to possible remote code execution via client update functionality. **CVE ID : CVE-2020-8289**		
Improper Privilege Management	27-Dec-20	4.6	Backblaze for Windows and Backblaze for macOS before 7.0.0.439 suffer from improper privilege management in `bztransmit` helper due to lack of permission handling and validation before creation of client update directories allowing for local escalation of privilege via rogue client update binary. **CVE ID : CVE-2020-8290**	N/A	A-BAC-BACK-040121/36
bigprof					
online_invoicing_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	BigProf Online Invoicing System before 3.1 fails to correctly sanitize an XSS payload when a user registers using the self-registration functionality. As such, an attacker can input a crafted payload that will execute upon the application's administrator browsing the registered users' list. Once the arbitrary Javascript is executed in the context of	N/A	A-BIG-ONLI-040121/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the admin, this will cause the attacker to gain administrative privileges, effectively leading into an application takeover. This affects app/membership_signup.php and app/admin/pageViewMembers.php. **CVE ID : CVE-2020-35676**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	3.5	BigProf Online Invoicing System before 4.0 fails to adequately sanitize fields for HTML characters upon an administrator using admin/pageEditGroup.php to create a new group, resulting in Stored XSS. The caveat here is that an attacker would need administrative privileges in order to create the payload. One might think this completely mitigates the privilege-escalation impact as there is only one high-privileged role. However, it was discovered that the endpoint responsible for creating the group lacks CSRF protection. **CVE ID : CVE-2020-35677**	N/A	A-BIG-ONLI-040121/38
bilanc					
bilanc					
Improper Neutralization of Special	21-Dec-20	7.5	An issue was discovered in Programi 014 31.01.2020. It has multiple SQL	N/A	A-BIL-BILA-040121/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			injection vulnerabilities. **CVE ID : CVE-2020-11717**		
Cleartext Transmission of Sensitive Information	23-Dec-20	5.8	An issue was discovered in Programi Bilanc build 007 release 014 31.01.2020 and below. Its software-update packages are downloaded via cleartext HTTP. **CVE ID : CVE-2020-11718**	N/A	A-BIL-BILA-040121/40
Inadequate Encryption Strength	23-Dec-20	5	An issue was discovered in Programi Bilanc build 007 release 014 31.01.2020 and possibly below. It relies on broken encryption with a weak and guessable static encryption key. **CVE ID : CVE-2020-11719**	N/A	A-BIL-BILA-040121/41
Use of Hard-coded Credentials	23-Dec-20	7.5	An issue was discovered in Programi Bilanc build 007 release 014 31.01.2020 and possibly below. During the installation, it sets up administrative access by default with the account admin and password 0000. After the installation, users/admins are not prompted to change this password. **CVE ID : CVE-2020-11720**	N/A	A-BIL-BILA-040121/42
Use of Hard-coded Credentials	21-Dec-20	5	Programi Bilanc Build 007 Release 014 31.01.2020 supplies a .exe file containing several	N/A	A-BIL-BILA-040121/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardcoded credentials to different servers that allow remote attackers to gain access to the complete infrastructure including the website, update server, and external issue tracking tools. **CVE ID : CVE-2020-8995**		
Bitdefender					
hypervisor_introspection					
Improper Input Validation	17-Dec-20	2.1	Lack of validation on data read from guest memory in IntPeGetDirectory, IntPeParseUnwindData, IntLogExceptionRecord, IntKsymExpandSymbol and IntLixTaskDumpTree may lead to out-of-bounds read or it could cause DoS due to integer-overflor (IntPeGetDirectory), TOCTOU (IntPeParseUnwindData) or insufficient validations. **CVE ID : CVE-2020-15292**	N/A	A-BIT-HYPE-040121/44
Improper Input Validation	17-Dec-20	2.1	Memory corruption in IntLixCrashDumpDmesg, IntLixTaskFetchCmdLine, IntLixFileReadDentry and IntLixFileGetPath due to insufficient guest-data input validation may lead to denial of service conditions. **CVE ID : CVE-2020-15293**	N/A	A-BIT-HYPE-040121/45
N/A	17-Dec-20	4.4	Compiler Optimization Removal or Modification of	N/A	A-BIT-HYPE-040121/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security-critical Code vulnerability in IntPeParseUnwindData() results in multiple dereferences to the same pointer. If the pointer is located in memory-mapped from the guest space, this may cause a race-condition where the generated code would dereference the same address twice, thus obtaining different values, which may lead to arbitrary code execution. This issue affects: Bitdefender Hypervisor Introspection versions prior to 1.132.2. **CVE ID : CVE-2020-15294**		
bloofoxcms_project					
bloofoxcms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Dec-20	4	bloofoxCMS 0.5.2.1 allows admins to upload arbitrary .php files (with "Content-Type: application/octet-stream") to ../media/images/ via the admin/index.php?mode=tools&page=upload URI, aka directory traversal. **CVE ID : CVE-2020-35709**	N/A	A-BLO-BLOO-040121/47
Bouncycastle					
legion-of-the-bouncy-castle-java-crytography-api					
N/A	18-Dec-20	7.5	An issue was discovered in Legion of the Bouncy Castle BC Java 1.65 and 1.66. The	N/A	A-BOU-LEGI-040121/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OpenBSDBCrypt.checkPassword utility method compared incorrect data when checking the password, allowing incorrect passwords to indicate they were matching with previously hashed ones that were different. **CVE ID : CVE-2020-28052**		
browserup					
browserup_proxy					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-Dec-20	7.5	BrowserUp Proxy allows you to manipulate HTTP requests and responses, capture HTTP content, and export performance data as a HAR file. BrowserUp Proxy works well as a standalone proxy server, but it is especially useful when embedded in Selenium tests. A Server-Side Template Injection was identified in BrowserUp Proxy enabling attackers to inject arbitrary Java EL expressions, leading to unauthenticated Remote Code Execution (RCE) vulnerability. This has been patched in version 2.1.2. **CVE ID : CVE-2020-26282**	https://github.com/browserup/browserup-proxy/security/advisories/GHSA-wmfg-55f9-j8hq	A-BRO-BROW-040121/49
Cmsmadesimple					
cms_made_simple					
Improper	17-Dec-20	4.3	Cross Site Scripting (XSS)	N/A	A-CMS-CMS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in the Showtime2 Slideshow module in CMS Made Simple (CMSMS) 2.2.4. **CVE ID : CVE-2020-20138**		040121/50
coastercms					
coastercms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-20	3.5	Coastercms v5.8.18 is affected by cross-site Scripting (XSS). A user can steal a cookie and make the user redirect to any malicious website because it is trigged on the main home page of the product/application. **CVE ID : CVE-2020-35275**	N/A	A-COA-COAS-040121/51
connection-tester_project					
connection-tester					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-20	7.5	This affects the package connection-tester before 0.2.1. The injection point is located in line 15 in index.js. The following PoC demonstrates the vulnerability: **CVE ID : CVE-2020-7781**	https://github.com/skoranga/node-connection-tester/pull/10, https://snyk.io/vuln/SNYK-JS-CONNECTIONTESTER-1048337	A-CON-CONN-040121/52
crk					
business_platform					
Improper Neutralization of Special	23-Dec-20	7.5	CRK Business Platform <= 2019.1 allows can inject SQL statements against the	N/A	A-CRK-BUSI-040121/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			DB on any path using the 'strSessao' parameter. **CVE ID : CVE-2020-13968**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-20	4.3	CRK Business Platform <= 2019.1 allows reflected XSS via erro.aspx on 'CRK', 'IDContratante', 'Erro', or 'Mod' parameter. This is path-independent. **CVE ID : CVE-2020-13969**	N/A	A-CRK-BUSI-040121/54
crossbar					
autobahn					
URL Redirection to Untrusted Site ('Open Redirect')	27-Dec-20	5.8	Autobahn|Python before 20.12.3 allows redirect header injection. **CVE ID : CVE-2020-35678**	https://autobahn.readthedocs.io/en/latest/changelog.html, https://github.com/crossbario/autobahn-python/pull/1439, https://pypi.org/project/autobahn/20.12.3/	A-CRO-AUTO-040121/55
cxuu					
cxuucms					
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-Dec-20	4.3	CXUUCMS V3 allows class="layui-input" XSS. **CVE ID : CVE-2020-29249**	N/A	A-CXU-CXUU-040121/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Dec-20	4.3	CXUUCMS V3 allows XSS via the first and third input fields to /public/admin.php. **CVE ID : CVE-2020-29250**	N/A	A-CXU-CXUU-040121/57
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Dec-20	3.5	CXUUCMS V3 3.1 is affected by a reflected XSS vulnerability that allows remote attackers to inject arbitrary web script or HTML via the imgurl parameter of admin.php?c=content&a=add. **CVE ID : CVE-2020-35346**	N/A	A-CXU-CXUU-040121/58
Cross-Site Request Forgery (CSRF)	26-Dec-20	4.3	CXUUCMS V3 3.1 has a CSRF vulnerability that can add an administrator account via admin.php?c=adminuser&a=add. **CVE ID : CVE-2020-35347**	N/A	A-CXU-CXUU-040121/59
Dart					
http					
N/A	24-Dec-20	4.3	An issue was discovered in the http package through 0.12.2 for Dart. If the attacker controls the HTTP method and the app is using Request directly, it's possible to achieve CRLF injection in an HTTP request. **CVE ID : CVE-2020-35669**	N/A	A-DAR-HTTP-040121/60
datatables					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
datatables.net					
Improper Input Validation	16-Dec-20	7.5	All versions of package datatables.net are vulnerable to Prototype Pollution due to an incomplete fix for https://snyk.io/vuln/SNYK-JS-DATATABLESNET-598806. **CVE ID : CVE-2020-28458**	N/A	A-DAT-DATA-040121/61
date-and-time_project					
date-and-time					
Uncontrolled Resource Consumption	28-Dec-20	5	date-and-time is an npm package for manipulating date and time. In date-and-time before version 0.14.2, there a regular expression involved in parsing which can be exploited to to cause a denial of service. This is fixed in version 0.14.2. **CVE ID : CVE-2020-26289**	https://github.com/knowledgecode/date-and-time/security/advisories/GHSA-r92x-f52r-x54g	A-DAT-DATE-040121/62
daybydaycrm					
daybyday					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Dec-20	3.5	Daybyday 2.1.0 allows stored XSS via the Title parameter to the New Lead screen. **CVE ID : CVE-2020-35704**	N/A	A-DAY-DAYB-040121/63
Improper Neutralization of Input During Web Page Generation ('Cross-site	25-Dec-20	3.5	Daybyday 2.1.0 allows stored XSS via the Name parameter to the New User screen. **CVE ID : CVE-2020-35705**	N/A	A-DAY-DAYB-040121/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Dec-20	3.5	Daybyday 2.1.0 allows stored XSS via the Title parameter to the New Project screen. **CVE ID : CVE-2020-35706**	N/A	A-DAY-DAYB-040121/65
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Dec-20	3.5	Daybyday 2.1.0 allows stored XSS via the Company Name parameter to the New Client screen. **CVE ID : CVE-2020-35707**	N/A	A-DAY-DAYB-040121/66
dbdeployer					
dbdeployer					
Improper Link Resolution Before File Access ('Link Following')	21-Dec-20	4	DBdeployer is a tool that deploys MySQL database servers easily. In DBdeployer before version 1.58.2, users unpacking a tarball may use a maliciously packaged tarball that contains symlinks to files external to the target. In such scenario, an attacker could induce dbdeployer to write into a system file, thus altering the computer defenses. For the attack to succeed, the following factors need to contribute: 1) The user is logged in as root. While dbdeployer is usable as root, it was designed to run as unprivileged user. 2) The user has taken a	https://github.com/datacharmer/dbdeployer/security/advisories/GHSA-47wr-426j-fr82	A-DBD-DBDE-040121/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tarball from a non secure source, without testing the checksum. When the tarball is retrieved through dbdeployer, the checksum is compared before attempting to unpack. This has been fixed in version 1.58.2. **CVE ID : CVE-2020-26277**		
deep-set_project					
deep-set					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'deep-set' versions 1.0.0 through 1.0.1 allows attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28276**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28276	A-DEE-DEEP-040121/68
Dell					
bsafe_micro_edition_suite					
Unchecked Return Value	16-Dec-20	5	Dell BSAFE Micro Edition Suite, versions prior to 4.5, are vulnerable to an Unchecked Return Value Vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability to modify and corrupt the encrypted data. **CVE ID : CVE-2020-5359**	N/A	A-DEL-BSAF-040121/69
Out-of-bounds Read	16-Dec-20	5	Dell BSAFE Micro Edition Suite, versions prior to 4.5, are vulnerable to a Buffer Under-Read Vulnerability. An unauthenticated remote	N/A	A-DEL-BSAF-040121/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could potentially exploit this vulnerability resulting in undefined behaviour, or a crash of the affected systems. **CVE ID : CVE-2020-5360**		
dext5					
dext5upload					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Dec-20	5	DEXT5Upload 2.7.1262310 and earlier is affected by Directory Traversal in handler/dext5handler.jsp. This could allow remote files to be downloaded via a dext5CMD=downloadRequest action with traversal in the fileVirtualPath parameter (the attacker must provide the correct fileOrgName value). **CVE ID : CVE-2020-35362**	N/A	A-DEX-DEXT-040121/71
Docker					
composer					
Missing Authentication for Critical Function	17-Dec-20	10	The official composer docker images before 1.8.3 contain a blank password for a root user. System using the composer docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35184**	N/A	A-DOC-COMP-040121/72
ghost_alpine_docker_image					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	17-Dec-20	10	The official ghost docker images before 2.16.1-alpine (Alpine specific) contain a blank password for a root user. System using the ghost docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35185**	N/A	A-DOC-GHOS-040121/73
adminer					
Missing Authentication for Critical Function	17-Dec-20	10	The official adminer docker images before 4.7.0-fastcgi contain a blank password for a root user. System using the adminer docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35186**	N/A	A-DOC-ADMI-040121/74
haproxy_docker_image					
Missing Authentication for Critical Function	17-Dec-20	10	The official haproxy docker images before 1.8.18-alpine (Alpine specific) contain a blank password for a root user. System using the haproxy docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	N/A	A-DOC-HAPR-040121/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35195		
rabbitmq_docker_image					
Missing Authentication for Critical Function	17-Dec-20	10	The official rabbitmq docker images before 3.7.13-beta.1-management-alpine (Alpine specific) contain a blank password for a root user. System using the rabbitmq docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35196**	N/A	A-DOC-RABB-040121/76
memcached_docker_image					
Missing Authentication for Critical Function	17-Dec-20	10	The official memcached docker images before 1.5.11-alpine (Alpine specific) contain a blank password for a root user. System using the memcached docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35197**	N/A	A-DOC-MEMC-040121/77
Dolibarr					
dolibarr					
Improper Neutralization of Special Elements used	23-Dec-20	9	Dolibarr 12.0.3 is vulnerable to authenticated Remote Code Execution. An	N/A	A-DOL-DOLI-040121/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in a Command ('Command Injection')			attacker who has the access the admin dashboard can manipulate the backup function by inserting a payload into the filename for the zipfilename_template parameter to admin/tools/dolibarr_export.php. **CVE ID : CVE-2020-35136**		
Dotcms					
dotcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-20	3.5	DotCMS Add Template with admin panel 20.11 is affected by cross-site Scripting (XSS) to gain remote privileges. An attacker could compromise the security of a website or web application through a stored XSS attack and stealing cookies using XSS. **CVE ID : CVE-2020-35274**	N/A	A-DOT-DOTC-040121/79
Drupal					
drupal_docker_images					
Missing Authentication for Critical Function	17-Dec-20	10	The official drupal docker images before 8.5.10-fpm-alpine (Alpine specific) contain a blank password for a root user. System using the drupal docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	N/A	A-DRU-DRUP-040121/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35191		
dset_project					
dset					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'dset' versions 1.0.0 through 2.0.1 allows attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28277**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28277	A-DSE-DSET-040121/81
egavilanmedia					
under_construction_page_with_cpanel					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Dec-20	7.5	EGavilan Media Under Construction page with cPanel 1.0 contains a SQL injection vulnerability. An attacker can gain Admin Panel access using malicious SQL injection queries to perform remote arbitrary code execution. **CVE ID : CVE-2020-29472**	N/A	A-EGA-UNDE-040121/82
egm_address_book					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Dec-20	7.5	EGavilan Media EGM Address Book 1.0 contains a SQL injection vulnerability. An attacker can gain Admin Panel access using malicious SQL injection queries to perform remote arbitrary code execution. **CVE ID : CVE-2020-29474**	N/A	A-EGA-EGM_-040121/83
user_registration_and_login_system_with_admin_panel					
Improper Neutralization	23-Dec-20	4.3	Cross Site Scripting (XSS) vulnerability via the 'Full	N/A	A-EGA-USER-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			Name' parameter in the User Registration section of User Registration & Login System with Admin Panel 1.0. **CVE ID : CVE-2020-35252**		040121/84
user_registration_\&_login_system_with_admin_panel					
Cross-Site Request Forgery (CSRF)	21-Dec-20	6	EgavilanMedia User Registration & Login System with Admin Panel 1.0 is affected by Cross Site Request Forgery (CSRF) to remotely gain privileges in the User Profile panel. An attacker can update any user's account. **CVE ID : CVE-2020-35273**	N/A	A-EGA-USER-040121/85
ecm_address_book					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-20	7.5	EgavilanMedia ECM Address Book 1.0 is affected by SQL injection. An attacker can bypass the Admin Login panel through SQLi and get Admin access and add or remove any user. **CVE ID : CVE-2020-35276**	N/A	A-EGA-ECM_-040121/86
Epson					
epsonnet_setupmanager					
Uncontrolled Search Path Element	24-Dec-20	9.3	Untrusted search path vulnerability in self-extracting files created by EpsonNet SetupManager versions 2.2.14 and earlier, and Offirio SynergyWare PrintDirector versions 1.6x/1.6y and earlier allows an attacker to gain	N/A	A-EPS-EPSO-040121/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2020-5681**		
offirio_synergyware_printdirector					
Uncontrolled Search Path Element	24-Dec-20	9.3	Untrusted search path vulnerability in self-extracting files created by EpsonNet SetupManager versions 2.2.14 and earlier, and Offirio SynergyWare PrintDirector versions 1.6x/1.6y and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2020-5681**	N/A	A-EPS-OFFI-040121/88
Esri					
arcgis_server					
Server-Side Request Forgery (SSRF)	26-Dec-20	9.3	Esri ArcGIS Server before 10.8 is vulnerable to SSRF in some configurations. **CVE ID : CVE-2020-35712**	N/A	A-ESR-ARCG-040121/89
F5					
big-ip_carrier-grade_nat					
N/A	24-Dec-20	4.3	On BIG-IP LTM/CGNAT version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.5, when processing NAT66 traffic with Port Block Allocation (PBA) mode and SP-DAG enabled, and dag-ipv6-prefix-len configured with a value less than the default of 128, an	N/A	A-F5-BIG--040121/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic pattern may cause the Traffic Management Microkernel (TMM) to restart. **CVE ID : CVE-2020-27720**		
big-ip_access_policy_manager					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/91
N/A	24-Dec-20	7.8	On versions 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.5, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, when a BIG-IP APM virtual server processes traffic of an undisclosed nature, the Traffic Management Microkernel (TMM) stops responding and restarts. **CVE ID : CVE-2020-27716**	N/A	A-F5-BIG--040121/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/93
Uncontrolled Resource Consumption	24-Dec-20	3.5	In BIG-IP APM versions 15.0.0-15.0.1.3, 14.1.0-14.1.3, and 13.1.0-13.1.3.4,	N/A	A-F5-BIG--040121/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			under certain conditions, the VDI plugin does not observe plugin flow-control protocol causing excessive resource consumption. **CVE ID : CVE-2020-27722**		
N/A	24-Dec-20	5	In versions 14.1.0-14.1.3 and 13.1.0-13.1.3.4, a BIG-IP APM virtual server processing PingAccess requests may lead to a restart of the Traffic Management Microkernel (TMM) process. **CVE ID : CVE-2020-27723**	N/A	A-F5-BIG--040121/95
Uncontrolled Resource Consumption	24-Dec-20	4	In BIG-IP APM versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.4, 15.0.0-15.0.1.3, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, on systems running more than one TMM instance, authenticated VPN users may consume excessive resources by sending specially-crafted malicious traffic over the tunnel. **CVE ID : CVE-2020-27724**	N/A	A-F5-BIG--040121/96
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, and 12.1.0-12.1.5.2, a reflected cross-site scripting (XSS) vulnerability exists in the resource information page for authenticated users when a full webtop is	N/A	A-F5-BIG--040121/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured on the BIG-IP APM system. **CVE ID : CVE-2020-27726**		
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/98
URL Redirection to Untrusted Site ('Open Redirect')	24-Dec-20	5.8	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, an undisclosed link on the BIG-IP APM virtual server allows a malicious user to build an open redirect URI. **CVE ID : CVE-2020-27729**	N/A	A-F5-BIG--040121/99
big-ip_advanced_firewall_manager					
N/A	24-Dec-20	4.3	On the BIG-IP AFM version 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.5, when a Protocol Inspection Profile is attached to a FastL4 virtual server with the protocol field configured to either Other or All Protocols, the TMM may experience a restart if the profile processes non-	N/A	A-F5-BIG--040121/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TCP traffic. **CVE ID : CVE-2020-27714**		
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/101
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/102
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/103
big-ip_analytics					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via	N/A	A-F5-BIG--040121/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/105
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/106
big-ip_application_acceleration_manager					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/107
Improper Neutralization	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-	N/A	A-F5-BIG--040121/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**		
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/109
big-ip_application_security_manager					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/110
Uncontrolled Resource Consumption	24-Dec-20	5	When a BIG-IP ASM or Advanced WAF system running version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, or 11.6.1-11.6.5.2 processes requests with JSON payload, an unusually large	N/A	A-F5-BIG--040121/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number of parameters can cause excessive CPU usage in the BIG-IP ASM bd process. **CVE ID : CVE-2020-27718**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/112
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/113
N/A	24-Dec-20	4.3	On BIG-IP ASM & Advanced WAF versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, under certain conditions, Analytics, Visibility, and Reporting daemon (AVRD) may generate a core file and restart on the BIG-IP system when processing requests sent from mobile	N/A	A-F5-BIG--040121/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. **CVE ID : CVE-2020-27728**		
big-ip_domain_name_system					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/115
N/A	24-Dec-20	7.8	On BIG-IP DNS 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, and 12.1.0-12.1.5.2, undisclosed series of DNS requests may cause TMM to restart and generate a core file. **CVE ID : CVE-2020-27717**	N/A	A-F5-BIG--040121/116
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/117
N/A	24-Dec-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.1, 14.1.0-14.1.3, 13.1.0-13.1.3.5, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, in a BIG-IP DNS / BIG-IP LTM GSLB deployment, under certain circumstances, the BIG-IP DNS system may stop using	N/A	A-F5-BIG--040121/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a BIG-IP LTM virtual server for DNS response. **CVE ID : CVE-2020-27721**		
Missing Release of Resource after Effective Lifetime	24-Dec-20	3.5	In version 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2 of BIG-IP DNS, GTM, and Link Controller, zxfrd leaks memory when listing DNS zones. Zones can be listed via TMSH, iControl or SNMP; only users with access to those services can trigger this vulnerability. **CVE ID : CVE-2020-27725**	N/A	A-F5-BIG--040121/119
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/120
big-ip_fraud_protection_service					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon.	N/A	A-F5-BIG--040121/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27715		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/122
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/123
big-ip_global_traffic_manager					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/124
Improper Neutralization of Input During Web Page Generation	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an	N/A	A-F5-BIG--040121/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**		
N/A	24-Dec-20	4.3	In versions 16.0.0-16.0.0.1, 15.1.0-15.1.1, 14.1.0-14.1.3, 13.1.0-13.1.3.5, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, in a BIG-IP DNS / BIG-IP LTM GSLB deployment, under certain circumstances, the BIG-IP DNS system may stop using a BIG-IP LTM virtual server for DNS response. **CVE ID : CVE-2020-27721**	N/A	A-F5-BIG--040121/126
Missing Release of Resource after Effective Lifetime	24-Dec-20	3.5	In version 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2 of BIG-IP DNS, GTM, and Link Controller, zxfrd leaks memory when listing DNS zones. Zones can be listed via TMSH, iControl or SNMP; only users with access to those services can trigger this vulnerability. **CVE ID : CVE-2020-27725**	N/A	A-F5-BIG--040121/127
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user	N/A	A-F5-BIG--040121/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**		
big-ip_link_controller					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/130
Missing Release of Resource after Effective Lifetime	24-Dec-20	3.5	In version 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2 of BIG-IP DNS, GTM, and Link Controller, zxfrd leaks memory when listing DNS zones. Zones can be listed via TMSH, iControl or SNMP; only users with access to those services can trigger this vulnerability. **CVE ID : CVE-2020-27725**	N/A	A-F5-BIG--040121/131
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-	N/A	A-F5-BIG--040121/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**		
big-ip_local_traffic_manager					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/133
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/134
N/A	24-Dec-20	4.3	On BIG-IP LTM/CGNAT version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.5, when processing NAT66 traffic with Port Block Allocation (PBA) mode and SP-DAG enabled, and dag-ipv6-prefix-len configured with a value less than the	N/A	A-F5-BIG--040121/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default of 128, an undisclosed traffic pattern may cause the Traffic Management Microkernel (TMM) to restart. **CVE ID : CVE-2020-27720**		
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/136
big-ip_policy_enforcement_manager					
N/A	24-Dec-20	7.8	On BIG-IP 15.1.0-15.1.0.5 and 14.1.0-14.1.3, crafted TLS request to the BIG-IP management interface via port 443 can cause high (~100%) CPU utilization by the httpd daemon. **CVE ID : CVE-2020-27715**	N/A	A-F5-BIG--040121/137
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	24-Dec-20	4	On BIG-IP version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, and 13.1.0-13.1.3.4, when an authenticated administrative user installs RPMs using the iAppsLX REST installer, the BIG-IP system does not sufficiently validate user input, allowing the user read access to the filesystem. **CVE ID : CVE-2020-27727**	N/A	A-F5-BIG--040121/139
ssl_orchestrator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-SSL_-040121/140
big-ip_advanced_web_application_firewall					
Uncontrolled Resource Consumption	24-Dec-20	5	When a BIG-IP ASM or Advanced WAF system running version 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, or 11.6.1-11.6.5.2 processes requests with JSON payload, an unusually large number of parameters can cause excessive CPU usage in the BIG-IP ASM bd process. **CVE ID : CVE-2020-27718**	N/A	A-F5-BIG--040121/141

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/142
N/A	24-Dec-20	4.3	On BIG-IP ASM & Advanced WAF versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, under certain conditions, Analytics, Visibility, and Reporting daemon (AVRD) may generate a core file and restart on the BIG-IP system when processing requests sent from mobile devices. **CVE ID : CVE-2020-27728**	N/A	A-F5-BIG--040121/143
big-ip_ddos_hybrid_defender					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	On BIG-IP 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, and 14.1.0-14.1.3, a cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-27719**	N/A	A-F5-BIG--040121/144
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	17-Dec-20	6.8	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between	N/A	A-FAS-JACK-040121/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources.PerUserPoolDataSource. **CVE ID : CVE-2020-35490**		
Deserialization of Untrusted Data	17-Dec-20	6.8	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.dbcp2.datasources.SharedPoolDataSource. **CVE ID : CVE-2020-35491**	N/A	A-FAS-JACK-040121/146
Deserialization of Untrusted Data	27-Dec-20	6.8	FasterXML jackson-databind 2.x before 2.9.10.8 mishandles the interaction between serialization gadgets and typing, related to com.oracle.wls.shaded.org.apache.xalan.lib.sql.JNDIConnectionPool (aka embedded Xalan in org.glassfish.web/javax.servlet.jsp.jstl). **CVE ID : CVE-2020-35728**	N/A	A-FAS-JACK-040121/147
flamingo_project					
flamingo					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	26-Dec-20	7.5	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::updateUserTeamInfoInDbAndMemory. **CVE ID : CVE-2020-35242**	N/A	A-FLA-FLAM-040121/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Dec-20	7.5	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::updateUserInfoInDb. **CVE ID : CVE-2020-35243**	N/A	A-FLA-FLAM-040121/149
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Dec-20	7.5	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::addGroup. **CVE ID : CVE-2020-35244**	N/A	A-FLA-FLAM-040121/150
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Dec-20	7.5	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::addUser. **CVE ID : CVE-2020-35245**	N/A	A-FLA-FLAM-040121/151
flamingoim_project					
flamingoim					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Dec-20	5	Flamingo (aka FlamingoIM) through 2020-09-29 allows ../ directory traversal because the only ostensibly unpredictable part of a file-transfer request is an MD5 computation; however, this computation occurs on the client side, and the computation details can be easily determined because	N/A	A-FLA-FLAM-040121/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the product's source code is available. **CVE ID : CVE-2020-35284**		
flattenizer_project					
flattenizer					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'flattenizer' versions 0.0.5 through 1.0.5 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28279**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28279	A-FLA-FLAT-040121/153
fleetdm					
fleet					
Authentication Bypass by Spoofing	17-Dec-20	6.8	Fleet is an open source osquery manager. In Fleet before version 3.5.1, due to issues in Go's standard library XML parsing, a valid SAML response may be mutated by an attacker to modify the trusted document. This can result in allowing unverified logins from a SAML IdP. Users that configure Fleet with SSO login may be vulnerable to this issue. This issue is patched in 3.5.1. The fix was made using https://github.com/mattermost/xml-roundtrip-validator If upgrade to 3.5.1 is not possible, users should disable SSO authentication in Fleet.	https://github.com/fleetdm/fleet/security/advisories/GHSA-w3wf-cfx3-6gcx	A-FLE-FLEE-040121/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26276		
flexmonster					
pivot_table_\&_charts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	4.3	Cross Site Scripting (XSS) vulnerability in the Remote JSON component Under the Connect menu in Flexmonster Pivot Table & Charts 2.7.17. **CVE ID : CVE-2020-20139**	N/A	A-FLE-PIVO-040121/155
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	4.3	Cross Site Scripting (XSS) vulnerability in Remote Report component under the Open menu in Flexmonster Pivot Table & Charts 2.7.17. **CVE ID : CVE-2020-20140**	N/A	A-FLE-PIVO-040121/156
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	4.3	Cross Site Scripting (XSS) vulnerability in the To OLAP (XMLA) component Under the Connect menu in Flexmonster Pivot Table & Charts 2.7.17. **CVE ID : CVE-2020-20141**	N/A	A-FLE-PIVO-040121/157
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	4.3	Cross Site Scripting (XSS) vulnerability in the "To Remote CSV" component under "Open" Menu in Flexmonster Pivot Table & Charts 2.7.17. **CVE ID : CVE-2020-20142**	N/A	A-FLE-PIVO-040121/158
Foxitsoftware					
foxit_reader					
Access of Resource Using Incompatible Type ('Type	22-Dec-20	6.8	A type confusion vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF	N/A	A-FOX-FOXI-040121/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Confusion')			Reader, version 10.1.0.37527. A specially crafted PDF document can trigger an improper use of an object, resulting in memory corruption and arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability. **CVE ID : CVE-2020-13547**		
Use After Free	22-Dec-20	6.8	A use after free vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 10.1.0.37527. A specially crafted PDF document can trigger reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability. **CVE ID : CVE-2020-13557**	N/A	A-FOX-FOXI-040121/160
Use After Free	22-Dec-20	6.8	A use after free vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF	N/A	A-FOX-FOXI-040121/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Reader, version 10.1.0.37527. A specially crafted PDF document can trigger reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability. **CVE ID : CVE-2020-13560**		
Use After Free	22-Dec-20	6.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.0.37527. A specially crafted PDF document can trigger the reuse of previously free memory which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability. **CVE ID : CVE-2020-13570**	N/A	A-FOX-FOXI-040121/162
Freedesktop					
poppler					
Out-of-bounds Write	25-Dec-20	6.8	** DISPUTED ** DCTStream::getChars in	N/A	A-FRE-POPP-040121/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DCTStream.cc in Poppler 20.12.1 has a heap-based buffer overflow via a crafted PDF document. NOTE: later reports indicate that this only affects builds from Poppler git clones in late December 2020, not the 20.12.1 release. In this situation, it should NOT be considered a Poppler vulnerability. However, several third-party Open Source projects directly rely on Poppler git clones made at arbitrary times, and therefore the CVE remains useful to users of those projects. **CVE ID : CVE-2020-35702**		
freehtmldesigns					
site_offline					
Cross-Site Request Forgery (CSRF)	29-Dec-20	4.3	The site-offline plugin before 1.4.4 for WordPress lacks certain wp_create_nonce and wp_verify_nonce calls, aka CSRF. **CVE ID : CVE-2020-35773**	N/A	A-FRE-SITE-040121/164
gdatasoftware					
g_data					
Improper Privilege Management	28-Dec-20	7.5	An issue was discovered in G-Data before 25.5.9.25 using Symbolic links, it is possible to abuse the infected-file restore mechanism to achieve arbitrary write that leads	N/A	A-GDA-G_DA-040121/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to elevation of privileges. **CVE ID : CVE-2020-27172**		
getobject_project					
getobject					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'getobject' version 0.1.0 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28282**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28282	A-GET-GETO-040121/166
Gnome					
gdk-pixbuf					
Loop with Unreachable Exit Condition ('Infinite Loop')	26-Dec-20	4.3	GNOME gdk-pixbuf (aka GdkPixbuf) before 2.42.2 allows a denial of service (infinite loop) in lzw.c in the function write_indexes. if c->self_code equals 10, self->code_table[10].extends will assign the value 11 to c. The next execution in the loop will assign self->code_table[11].extends to c, which will give the value of 10. This will make the loop run infinitely. This bug can, for example, be triggered by calling this function with a GIF image with LZW compression that is crafted in a special way. **CVE ID : CVE-2020-29385**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=977166, https://gitlab.gnome.org/GNOME/gdk-pixbuf/-/issues/164, https://ubuntu.com/security/CVE-2020-29385	A-GNO-GDK--040121/167
gnome_display_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	28-Dec-20	4.4	A flaw was found in GDM in versions prior to 3.38.2.1. A race condition in the handling of session shutdown makes it possible to bypass the lock screen for a user that has autologin enabled, accessing their session without authentication. This is similar to CVE-2017-12164, but requires more difficult conditions to exploit. **CVE ID : CVE-2020-27837**	N/A	A-GNO-GNOM-040121/168
GNU					
binutils					
Out-of-bounds Write	27-Dec-20	6.8	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.35.1. A heap-based buffer over-read can occur in bfd_getl_signed_32 in libbfd.c because sh_entsize is not validated in _bfd_elf_slurp_secondary_reloc_section in elf.c. **CVE ID : CVE-2020-35448**	N/A	A-GNU-BINU-040121/169
gobby_project					
gobby					
NULL Pointer Dereference	26-Dec-20	5	Gobby 0.4.11 allows a NULL pointer dereference in the D-Bus handler for certain set_language calls. **CVE ID : CVE-2020-35450**	N/A	A-GOB-GOBB-040121/170
gohugo					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hugo					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-20	8.5	Hugo is a fast and Flexible Static Site Generator built in Go. Hugo depends on Go's `os/exec` for certain features, e.g. for rendering of Pandoc documents if these binaries are found in the system `%PATH%` on Windows. In Hugo before version 0.79.1, if a malicious file with the same name (`exe` or `bat`) is found in the current working directory at the time of running `hugo`, the malicious command will be invoked instead of the system one. Windows users who run `hugo` inside untrusted Hugo sites are affected. Users should upgrade to Hugo v0.79.1. Other than avoiding untrusted Hugo sites, there is no workaround. **CVE ID : CVE-2020-26284**	https://github.com/gohugoio/hugo/security/advisories/GHSA-8j34-9876-pvfq	A-GOH-HUGO-040121/171
Golang					
go					
NULL Pointer Dereference	17-Dec-20	5	A nil pointer dereference in the golang.org/x/crypto/ssh component through v0.0.0-20201203163018-be400aefbc4c for Go allows remote attackers to cause a denial of service against SSH servers. **CVE ID : CVE-2020-29652**	N/A	A-GOL-GO-040121/172

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
grafana					
grafana					
Misinterpretation of Input	21-Dec-20	10	A signature verification vulnerability exists in crewjam/saml. This flaw allows an attacker to bypass SAML Authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-27846**	N/A	A-GRA-GRAF-040121/173
hashicorp					
vault					
Information Exposure	17-Dec-20	5	HashiCorp Vault and Vault Enterprise allowed the enumeration of users via the LDAP auth method. Fixed in 1.5.6 and 1.6.1. **CVE ID : CVE-2020-35177**	https://discuss.hashicorp.com/t/hcsec-2020-25-vault-s-ldap-auth-method-allows-user-enumeration/18984, https://github.com/hashicorp/vault/blob/master/CHANGELOG.md#161	A-HAS-VAUL-040121/174
Missing Authentication for Critical Function	17-Dec-20	10	The official vault docker images before 0.11.6 contain a blank password for a root user. System using the vault docker	N/A	A-HAS-VAUL-040121/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35192**		
Improper Input Validation	17-Dec-20	5	HashiCorp Vault Enterprise's Sentinel EGP policy feature incorrectly allowed requests to be processed in parent and sibling namespaces. Fixed in 1.5.6 and 1.6.1. **CVE ID : CVE-2020-35453**	https://discuss.hashicorp.com/t/hcsec-2020-24-vault-enterprise-s-sentinel-egp-policies-may-impact-parent-or-sibling-namespaces/18983, https://github.com/hashicorp/vault/blob/master/CHANGELOG.md#161	A-HAS-VAUL-040121/176
hcltech					
domino					
Information Exposure Through an Error Message	22-Dec-20	5	HCL Domino v9, v10, v11 is susceptible to an Information Disclosure vulnerability in XPages due to improper error handling of user input. An unauthenticated attacker	N/A	A-HCL-DOMI-040121/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability to obtain information about the XPages software running on the Domino server. **CVE ID : CVE-2020-14270**		
Improper Input Validation	28-Dec-20	5	HCL Domino v10 and v11 is susceptible to a Denial of Service (DoS) vulnerability due to insufficient validation of input to its public API. An unauthenticated attacker could could exploit this vulnerability to crash the Domino server. **CVE ID : CVE-2020-14273**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0085947	A-HCL-DOMI-040121/178
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	HCL Verse v10 and v11 is susceptible to a Stored Cross-Site Scripting (XSS) vulnerability due to improper handling of message content. An unauthenticated remote attacker could exploit this vulnerability using specially-crafted markup to execute script in a victim's web browser within the security context of the hosting Web site and/or steal the victim's cookie-based authentication credentials. **CVE ID : CVE-2020-4080**	N/A	A-HCL-DOMI-040121/179
hcl_inotes					
N/A	21-Dec-20	4.3	HCL iNotes is susceptible to a Tabnabbing vulnerability caused by	N/A	A-HCL-HCL_-040121/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper sanitization of message content. A remote unauthenticated attacker could use this vulnerability to trick the end user into entering sensitive information such as credentials, e.g. as part of a phishing attack. **CVE ID : CVE-2020-14225**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	HCL iNotes v9, v10 and v11 is susceptible to a Stored Cross-Site Scripting (XSS) vulnerability due to improper handling of message content. An unauthenticated remote attacker could exploit this vulnerability using specially-crafted markup to execute script in a victim's web browser within the security context of the hosting Web site and/or steal the victim's cookie-based authentication credentials. **CVE ID : CVE-2020-14271**	N/A	A-HCL-HCL_-040121/181
bigfix_platform					
Cleartext Transmission of Sensitive Information	16-Dec-20	5	BigFix Inventory up to v10.0.2 does not set the secure flag for the session cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie. **CVE ID : CVE-2020-14248**	N/A	A-HCL-BIGF-040121/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Encryption of Sensitive Data	16-Dec-20	4.3	TLS-RSA cipher suites are not disabled in HCL BigFix Inventory up to v10.0.2. If TLS 2.0 and secure ciphers are not enabled then an attacker can passively record traffic and later decrypt it. **CVE ID : CVE-2020-14254**	N/A	A-HCL-BIGF-040121/183
notes					
Out-of-bounds Write	18-Dec-20	10	A vulnerability in the MIME message handling of the HCL Notes v9 client could potentially be exploited by an unauthenticated attacker resulting in a stack buffer overflow. This could allow a remote attacker to crash the Notes application or inject code into the system which would execute with the privileges of the currently logged-in user. **CVE ID : CVE-2020-14224**	N/A	A-HCL-NOTE-040121/184
N/A	18-Dec-20	9	A vulnerability in the input parameter handling of HCL Notes v9 could potentially be exploited by an authenticated attacker resulting in a stack buffer overflow. This could allow the attacker to crash the program or inject code into the system which would execute with the privileges of the currently logged in user. **CVE ID : CVE-2020-14232**	N/A	A-HCL-NOTE-040121/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hcltechsw					
hcl_inotes					
N/A	21-Dec-20	4.3	HCL iNotes is susceptible to a Tabnabbing vulnerability caused by improper sanitization of message content. A remote unauthenticated attacker could use this vulnerability to trick the end user into entering sensitive information such as credentials, e.g. as part of a phishing attack. **CVE ID : CVE-2020-14225**	N/A	A-HCL-HCL_-040121/186
hcl_client_application_access					
Out-of-bounds Write	22-Dec-20	6.5	A vulnerability in the input parameter handling of HCL Client Application Access v9 could potentially be exploited by an authenticated attacker resulting in a stack buffer overflow. This could allow the attacker to crash the program or inject code into the system which would execute with the privileges of the currently logged in user. **CVE ID : CVE-2020-14231**	N/A	A-HCL-HCL_-040121/187
hedgedoc					
hedgedoc					
Unrestricted Upload of File with Dangerous Type	29-Dec-20	5	HedgeDoc is a collaborative platform for writing and sharing markdown. In HedgeDoc before version 1.7.1 an	https://github.com/hedgedoc/hedgedoc/security/advis	A-HED-HEDG-040121/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker can upload arbitrary files to the upload storage backend including HTML, JS and PHP files. The problem is patched in HedgeDoc 1.7.1. You should however verify that your uploaded file storage only contains files that are allowed, as uploaded files might still be served. As workaround it's possible to block the `/uploadimage` endpoint on your instance using your reverse proxy. And/or restrict MIME-types and file names served from your upload file storage. **CVE ID : CVE-2020-26286**	ories/GHSA-wcr3-xhv7-8gxc	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Dec-20	4.3	HedgeDoc is a collaborative platform for writing and sharing markdown. In HedgeDoc before version 1.7.1 an attacker can inject arbitrary `script` tags in HedgeDoc notes using mermaid diagrams. Our content security policy prevents loading scripts from most locations, but `www.google-analytics.com` is allowed. Using Google Tag Manger it is possible to inject arbitrary JavaScript and execute it on page load. Depending on the	https://github.com/hedgedoc/hedgedoc/security/advisories/GHSA-g6w6-7xf9-m95p	A-HED-HEDG-040121/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration of the instance, the attacker may not need authentication to create or edit notes. The problem is patched in HedgeDoc 1.7.1. As a workaround one can disallow `www.google-analytics.com` in the `Content-Security-Policy` header. Note that other ways to leverage the `script` tag injection might exist. **CVE ID : CVE-2020-26287**		
HP					
systems_insight_manager					
N/A	18-Dec-20	7.5	A potential security vulnerability has been identified in HPE Systems Insight Manager (SIM) version 7.6. The vulnerability could be exploited to allow remote code execution. **CVE ID : CVE-2020-7200**	N/A	A-HP-SYST-040121/190
ilo_amplifier_pack					
N/A	18-Dec-20	7.5	A potential security vulnerability has been identified in HPE iLO Amplifier Pack server version 1.70. The vulnerability could be exploited to allow remote code execution. **CVE ID : CVE-2020-7203**	N/A	A-HP-ILO_-040121/191
Huawei					
cloudengine_1800v					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	24-Dec-20	5	CloudEngine 1800V versions V100R019C10SPC500 has a resource management error vulnerability. Remote unauthorized attackers could send specific types of messages to the device, resulting in the message received by the system can't be forwarded normally. **CVE ID : CVE-2020-9120**	N/A	A-HUA-CLOU-040121/192
imanager_neteco_6000					
N/A	24-Dec-20	7.2	There has a CSV injection vulnerability in iManager NetEco 6000 versions V600R021C00. An attacker with common privilege may exploit this vulnerability through some operations to inject the CSV files. Due to insufficient input validation of some parameters, the attacker can exploit this vulnerability to inject CSV files to the target device. **CVE ID : CVE-2020-9200**	N/A	A-HUA-IMAN-040121/193
Information Exposure	29-Dec-20	4	There is an information leak vulnerability in iManager NetEco 6000 versions V600R021C00. A module is lack of authentication. Attackers without access to the module can exploit this vulnerability to obtain extra information, leading	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-neteco-en	A-HUA-IMAN-040121/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to information leak. **CVE ID : CVE-2020-9208**		
te_mobile					
Insecure Storage of Sensitive Information	24-Dec-20	2.1	There is an information disclosure vulnerability in TE Mobile software versions V600R006C10,V600R006C10SPC100. Due to the improper storage of some information in certain specific scenario, the attacker can gain information in the victim's device to launch the attack, successful exploit could cause information disclosure. **CVE ID : CVE-2020-9202**	N/A	A-HUA-TE_M-040121/195
huorong					
internet_security					
Improper Privilege Management	26-Dec-20	7.5	Beijing Huorong Internet Security 5.0.55.2 allows a non-admin user to escalate privileges by injecting code into a process, and then waiting for a Huorong services restart or a system reboot. **CVE ID : CVE-2020-35364**	N/A	A-HUO-INTE-040121/196
IBM					
planning_analytics					
Cross-Site Request Forgery (CSRF)	18-Dec-20	4.3	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and	https://www.ibm.com/support/pages/node/6386492	A-IBM-PLAN-040121/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 188898. **CVE ID : CVE-2020-4764**		
sterling_file_gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186095. **CVE ID : CVE-2020-4658**	https://www.ibm.com/support/pages/node/6382416	A-IBM-STER-040121/198
security_key_lifecycle_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	3.5	IBM Security Key Lifecycle Manager 3.0.1 and 4.0 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: 190289. **CVE ID : CVE-2020-4845**	https://www.ibm.com/support/pages/node/6253781	A-IBM-SECU-040121/199
Information Exposure Through an	17-Dec-20	4	IBM Security Key Lifecycle Manager 3.0.1 and 4.0 could allow a remote	https://www.ibm.com/support/p	A-IBM-SECU-040121/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Error Message			attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 190290. **CVE ID : CVE-2020-4846**	ages/node/6253781	
security_secret_server					
URL Redirection to Untrusted Site ('Open Redirect')	21-Dec-20	5.8	IBM Security Secret Server 10.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 190044. **CVE ID : CVE-2020-4840**	https://www.ibm.com/support/pages/node/6336251	A-IBM-SECU-040121/201
Information Exposure	21-Dec-20	4.3	IBM Security Secret Server 10.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to	https://www.ibm.com/support/pages/node/6336251	A-IBM-SECU-040121/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain sensitive information using man in the middle techniques. IBM X-Force ID: 190045. **CVE ID : CVE-2020-4841**		
Information Exposure Through an Error Message	21-Dec-20	4	IBM Security Secret Server 10.6 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 190046. **CVE ID : CVE-2020-4842**	https://www.ibm.com/support/pages/node/6336251	A-IBM-SECU-040121/203
Cleartext Storage of Sensitive Information	21-Dec-20	4	IBM Security Secret Server 10.6 stores potentially sensitive information in config files that could be read by an authenticated user. IBM X-Force ID: 190048. **CVE ID : CVE-2020-4843**	https://www.ibm.com/support/pages/node/6250375	A-IBM-SECU-040121/204
db2					
N/A	23-Dec-20	2.1	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow local attacker to cause a denial of service inside the "DB2 Management Service". **CVE ID : CVE-2020-4642**	https://www.ibm.com/support/pages/node/6391652	A-IBM-DB2-040121/205
sterling_b2b_integrator					
Improper Neutralization of Input During	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition is	https://www.ibm.com/support/p	A-IBM-STER-040121/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			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: 186094. **CVE ID : CVE-2020-4657**	ages/node/6382414	
financial_transaction_manager					
Session Fixation	21-Dec-20	5.5	IBM Financial Transaction Manager 3.0.6 and 3.1.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 183328. **CVE ID : CVE-2020-4555**	https://www.ibm.com/support/pages/node/6388702, https://www.ibm.com/support/pages/node/6388704, https://www.ibm.com/support/pages/node/6388706, https://www.ibm.com/support/pages/node/6388708, https://www.ibm.com/support/pages/node/6388722	A-IBM-FINA-040121/207
content_navigator					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-20	3.5	IBM FileNet Content Manager and IBM Content Navigator 3.0.CD is vulnerable to stored 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: 188600. **CVE ID : CVE-2020-4757**	https://www.ibm.com/support/pages/node/6388806	A-IBM-CONT-040121/208
mq					
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	A-IBM-MQ-040121/209
business_automation_workflow					
Incorrect Authorization	21-Dec-20	5.5	IBM Automation Workstream Services 19.0.3, 20.0.1, 20.0.2, IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.6 could allow an authenticated user to obtain sensitive information or cuase a denial of service due to iimproper authorization	https://www.ibm.com/support/pages/node/6359463	A-IBM-BUSI-040121/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checking. IBM X-Force ID: 189445. **CVE ID : CVE-2020-4794**		
business_process_manager					
Incorrect Authorization	21-Dec-20	5.5	IBM Automation Workstream Services 19.0.3, 20.0.1, 20.0.2, IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.6 could allow an authenticated user to obtain sensitive information or cuase a denial of service due to iimproper authorization checking. IBM X-Force ID: 189445. **CVE ID : CVE-2020-4794**	https://www.ibm.com/support/pages/node/6359463	A-IBM-BUSI-040121/211
financial_transaction_manager_for_multiplatform					
Cross-Site Request Forgery (CSRF)	16-Dec-20	4.3	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID : CVE-2020-4904**	https://www.ibm.com/support/pages/node/6371260	A-IBM-FINA-040121/212
Information Exposure	16-Dec-20	4.3	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an remote attacker to obtain sensitive information, caused by a man in the	https://www.ibm.com/support/pages/node/6371260	A-IBM-FINA-040121/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			middle attack. By SSL striping, an attacker could exploit this vulnerability to obtain sensitive information. **CVE ID : CVE-2020-4905**		
Insecure Storage of Sensitive Information	16-Dec-20	2.1	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 allows web pages to be stored locally which can be read by another user on the system. **CVE ID : CVE-2020-4906**	https://www.ibm.com/support/pages/node/6371260	A-IBM-FINA-040121/214
Information Exposure Through an Error Message	16-Dec-20	5	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. **CVE ID : CVE-2020-4907**	https://www.ibm.com/support/pages/node/6371260	A-IBM-FINA-040121/215
Information Exposure	16-Dec-20	5	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 returns the product version and release information on the login dialog. This information could be used in further attacks against the system. **CVE ID : CVE-2020-4908**	https://www.ibm.com/support/pages/node/6371260	A-IBM-FINA-040121/216
automation_workstream_services					
Incorrect	21-Dec-20	5.5	IBM Automation	https://ww	A-IBM-AUTO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			Workstream Services 19.0.3, 20.0.1, 20.0.2, IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.6 could allow an authenticated user to obtain sensitive information or cuase a denial of service due to iimproper authorization checking. IBM X-Force ID: 189445. **CVE ID : CVE-2020-4794**	w.ibm.com /support/p ages/node/ 6359463	040121/217
loopback					
N/A	21-Dec-20	7.5	Loopback 8.0.0 contains a vulnerability that could allow an attacker to manipulate or pollute Javascript values and cause a denial of service or possibly execute code. IBM X-Force ID: 192706. **CVE ID : CVE-2020-4988**	N/A	A-IBM-LOOP-040121/218
influxdata					
telegraf					
Missing Authentication for Critical Function	17-Dec-20	10	The official telegraf docker images before 1.9.4-alpine (Alpine specific) contain a blank password for a root user. System using the telegraf docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password.	N/A	A-INF-TELE-040121/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35187		
chronograf					
Missing Authentication for Critical Function	17-Dec-20	10	The official chronograf docker images before 1.7.7-alpine (Alpine specific) contain a blank password for a root user. System using the chronograf docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35188**	N/A	A-INF-CHRO-040121/220
influxdb_docker_image					
Missing Authentication for Critical Function	17-Dec-20	10	The official influxdb docker images before 1.7.3-meta-alpine (Alpine specific) contain a blank password for a root user. System using the influxdb docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35194**	N/A	A-INF-INFL-040121/221
Intelliants					
subrion_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-Dec-20	4.3	Subrion CMS 4.2.1 is affected by: Cross Site Scripting (XSS) through the avatar[path] parameter in a POST request to the /_core/profile/ URI.	N/A	A-INT-SUBR-040121/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2020-35437**		
Irfanview					
irfanview					
Unrestricted Upload of File with Dangerous Type	16-Dec-20	5	irfanView 4.56 contains an error processing parsing files of type .pcx. Which leads to out-of-bounds writing at i_view32+0xdb60. **CVE ID : CVE-2020-35133**	N/A	A-IRF-IRFA-040121/223
jaws_project					
jaws					
Unrestricted Upload of File with Dangerous Type	23-Dec-20	6.5	Jaws through 1.8.0 allows remote authenticated administrators to execute arbitrary code via crafted use of admin.php?reqGadget=Components&reqAction=InstallGadget&comp=FileBrowser and admin.php?reqGadget=FileBrowser&reqAction=Files to upload a .php file. NOTE: this is unrelated to the JAWS (aka Job Access With Speech) product. **CVE ID : CVE-2020-35656**	N/A	A-JAW-JAWS-040121/224
Unrestricted Upload of File with Dangerous Type	23-Dec-20	6.5	Jaws through 1.8.0 allows remote authenticated administrators to execute arbitrary code via crafted use of UploadTheme to upload a theme ZIP archive containing a .php file that is able to execute OS commands. NOTE: this is unrelated to the JAWS (aka	N/A	A-JAW-JAWS-040121/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Job Access With Speech) product. **CVE ID : CVE-2020-35657**		
jiransecurity					
spamsniper					
Out-of-bounds Write	27-Dec-20	7.5	Spamsniper 5.0 ~ 5.2.7 contain a stack-based buffer overflow vulnerability caused by improper boundary checks when parsing MAIL FROM command. It leads remote attacker to execute arbitrary code via crafted packet. **CVE ID : CVE-2020-7845**	N/A	A-JIR-SPAM-040121/226
Joomla					
joomla\!					
N/A	28-Dec-20	5	An issue was discovered in Joomla! 2.5.0 through 3.9.22. The autosuggestion feature of com_finder did not respect the access level of the corresponding terms. **CVE ID : CVE-2020-35610**	N/A	A-JOO-JOOM-040121/227
Information Exposure	28-Dec-20	5	An issue was discovered in Joomla! 2.5.0 through 3.9.22. The globlal configuration page does not remove secrets from the HTML output, disclosing the current values. **CVE ID : CVE-2020-35611**	N/A	A-JOO-JOOM-040121/228
Improper Limitation of a	28-Dec-20	5	An issue was discovered in Joomla! 2.5.0 through	N/A	A-JOO-JOOM-040121/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			3.9.22. The folder parameter of mod_random_image lacked input validation, leading to a path traversal vulnerability. **CVE ID : CVE-2020-35612**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Dec-20	7.5	An issue was discovered in Joomla! 3.0.0 through 3.9.22. Improper filter blacklist configuration leads to a SQL injection vulnerability in the backend user list. **CVE ID : CVE-2020-35613**	N/A	A-JOO-JOOM-040121/230
Information Exposure	28-Dec-20	5	An issue was discovered in Joomla! 3.9.0 through 3.9.22. Improper handling of the username leads to a user enumeration attack vector in the backend login page. **CVE ID : CVE-2020-35614**	N/A	A-JOO-JOOM-040121/231
Cross-Site Request Forgery (CSRF)	28-Dec-20	6.8	An issue was discovered in Joomla! 2.5.0 through 3.9.22. A missing token check in the emailexport feature of com_privacy causes a CSRF vulnerability. **CVE ID : CVE-2020-35615**	N/A	A-JOO-JOOM-040121/232
Improper Input Validation	28-Dec-20	5	An issue was discovered in Joomla! 1.7.0 through 3.9.22. Lack of input validation while handling ACL rulesets can cause write ACL violations. **CVE ID : CVE-2020-35616**	N/A	A-JOO-JOOM-040121/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jsonpickle_project					
jsonpickle					
Deserialization of Untrusted Data	17-Dec-20	7.5	** DISPUTED ** jsonpickle through 1.4.1 allows remote code execution during deserialization of a malicious payload through the decode() function. Note: It has been argued that this is expected and clearly documented behaviour. pickle is known to be capable of causing arbitrary code execution, and must not be used with un-trusted data. **CVE ID : CVE-2020-22083**	N/A	A-JSO-JSON-040121/234
Jupyter					
jupyter_server					
URL Redirection to Untrusted Site ('Open Redirect')	21-Dec-20	5.8	The Jupyter Server provides the backend (i.e. the core services, APIs, and REST endpoints) for Jupyter web applications like Jupyter notebook, JupyterLab, and Voila. In Jupyter Server before version 1.1.1, an open redirect vulnerability could cause the jupyter server to redirect the browser to a different malicious website. All jupyter servers running without a base_url prefix are technically affected, however, these maliciously crafted links can only be reasonably made for known jupyter	https://github.com/jupyter-server/jupyter_server/security/advisories/GHSA-9f66-54xg-pc2c	A-JUP-JUPY-040121/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server hosts. A link to your jupyter server may *appear* safe, but ultimately redirect to a spoofed server on the public internet. This same vulnerability was patched in upstream notebook v5.7.8. This is fixed in jupyter_server 1.1.1. If upgrade is not available, a workaround can be to run your server on a url prefix: "jupyter server --ServerApp.base_url=/jupyter/". **CVE ID : CVE-2020-26275**		
Kepware					
linkmaster					
Incorrect Default Permissions	18-Dec-20	7.2	A privilege escalation vulnerability exists in Kepware LinkMaster 3.0.94.0. In its default configuration, an attacker can globally overwrite service configuration to execute arbitrary code with NT SYSTEM privileges. **CVE ID : CVE-2020-13535**	N/A	A-KEP-LINK-040121/236
kitty_project					
kitty					
N/A	21-Dec-20	7.5	The Graphics Protocol feature in graphics.c in kitty before 0.19.3 allows remote attackers to execute arbitrary code because a filename	N/A	A-KIT-KITT-040121/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			containing special characters can be included in an error message. **CVE ID : CVE-2020-35605**		
klogserver					
klog_server					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Dec-20	10	KLog Server 2.4.1 allows OS command injection via shell metacharacters in the actions/authenticate.php user parameter. **CVE ID : CVE-2020-35729**	N/A	A-KLO-KLOG-040121/238
Kong					
kong_alpine_docker_image					
Missing Authentication for Critical Function	17-Dec-20	10	The official kong docker images before 1.0.2-alpine (Alpine specific) contain a blank password for a root user. System using the kong docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35189**	N/A	A-KON-KONG-040121/239
Kronos					
web_time_and_attendance					
Improper Restriction of XML External Entity Reference ('XXE')	21-Dec-20	9.3	An XXE attack can occur in Kronos WebTA 5.0.4 when SAML is used. **CVE ID : CVE-2020-35604**	N/A	A-KRO-WEB_-040121/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libnested_project					
libnested					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'libnested' versions 0.0.0 through 1.5.0 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28283**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28284	A-LIB-LIBN-040121/241
library_management_system_project					
library_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Dec-20	7.5	SourceCodester Library Management System 1.0 is affected by SQL Injection allowing an attacker to bypass the user authentication and impersonate any user on the system. **CVE ID : CVE-2020-28073**	N/A	A-LIB-LIBR-040121/242
liftoffsoftware					
gateone					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Dec-20	5	GateOne 1.1 allows arbitrary file download without authentication via /downloads/.. directory traversal because os.path.join is misused. **CVE ID : CVE-2020-35736**	N/A	A-LIF-GATE-040121/243
limitloginattempts					
limit_login_attempts_reloaded					
Improper Neutralization of Input During Web Page	21-Dec-20	3.5	The limit-login-attempts-reloaded plugin before 2.17.4 for WordPress allows wp-admin/options-	N/A	A-LIM-LIMI-040121/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			general.php?page=limit-login-attempts&tab= XSS. A malicious user can cause an administrator user to supply dangerous content to the vulnerable page, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. **CVE ID : CVE-2020-35589**		
Improper Restriction of Excessive Authentication Attempts	21-Dec-20	5	LimitLoginAttempts.php in the limit-login-attempts-reloaded plugin before 2.17.4 for WordPress allows a bypass of (per IP address) rate limits because the X-Forwarded-For header can be forged. When the plugin is configured to accept an arbitrary header for the client source IP address, a malicious user is not limited to perform a brute force attack, because the client IP header accepts any arbitrary string. When randomizing the header input, the login count does not ever reach the maximum allowed retries. **CVE ID : CVE-2020-35590**	N/A	A-LIM-LIMI-040121/245
Linuxfoundation					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dex					
Improper Verification of Cryptographic Signature	28-Dec-20	6.8	Dex is a federated OpenID Connect provider written in Go. In Dex before version 2.27.0 there is a critical set of vulnerabilities which impacts users leveraging the SAML connector. The vulnerabilities enables potential signature bypass due to issues with XML encoding in the underlying Go library. The vulnerabilities have been addressed in version 2.27.0 by using the xml-roundtrip-validator from Mattermost (see related references). **CVE ID : CVE-2020-26290**	https://github.com/dexidp/dex/security/advisories/GHSA-m9hp-7r99-94h5	A-LIN-DEX-040121/246
osquery					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-20	3.6	osquery is a SQL powered operating system instrumentation, monitoring, and analytics framework. In osquery before version 4.6.0, by using sqlite's ATTACH verb, someone with administrative access to osquery can cause reads and writes to arbitrary sqlite databases on disk. This _does_ allow arbitrary files to be created, but they will be sqlite databases. It does not appear to allow existing non-sqlite files to be overwritten. This has been patched in osquery	https://github.com/osquery/osquery/security/advisories/GHSA-4g56-2482-x7q8	A-LIN-OSQU-040121/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.6.0. There are several mitigating factors and possible workarounds. In some deployments, the people with access to these interfaces may be considered administrators. In some deployments, configuration is managed by a central tool. This tool can filter for the `ATTACH` keyword. osquery can be run as non-root user. Because this also limits the desired access levels, this requires deployment specific testing and configuration. **CVE ID : CVE-2020-26273**		
indy-node					
Improper Verification of Cryptographic Signature	24-Dec-20	5	Hyperledger Indy Node is the server portion of a distributed ledger purpose-built for decentralized identity. In Hyperledger Indy before version 1.12.4, there is lack of signature verification on a specific transaction which enables an attacker to make certain unauthorized alterations to the ledger. Updating a DID with a nym transaction will be written to the ledger if neither ROLE or VERKEY are being changed, regardless of sender. A malicious DID with no particular role can ask an	https://github.com/hyperledger/indy-node/security/advisories/GHSA-wh2w-39f4-rpv2	A-LIN-INDY-040121/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update for another DID (but cannot modify its verkey or role). This is bad because 1) Any DID can write a nym transaction to the ledger (i.e., any DID can spam the ledger with nym transactions), 2) Any DID can change any other DID's alias, 3) The update transaction modifies the ledger metadata associated with a DID. **CVE ID : CVE-2020-11093**		
linux-pam					
linux-pam					
Improper Authentication	18-Dec-20	10	A flaw was found in Linux-Pam in versions prior to 1.5.1 in the way it handle empty passwords for non-existing users. When the user doesn't exist PAM try to authenticate with root and in the case of an empty password it successfully authenticate. **CVE ID : CVE-2020-27780**	N/A	A-LIN-LINU-040121/249
Litespeedtech					
litespeed_cache					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Dec-20	4.3	A cross-site scripting (XSS) vulnerability in the LiteSpeed Cache plugin before 3.6.1 for WordPress can be exploited via the Server IP setting. **CVE ID : CVE-2020-29172**	https://wordpress.org/plugins/litespeed-cache/#developers	A-LIT-LITE-040121/250
logrhythm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
platform_manager					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Dec-20	10	LogRhythm Platform Manager 7.4.9 allows Command Injection. To exploit this, an attacker can inject arbitrary program names and arguments into a WebSocket. These are forwarded to any remote server with a LogRhythm Smart Response agent installed. By default, the commands are run with LocalSystem privileges. **CVE ID : CVE-2020-25094**	N/A	A-LOG-PLAT-040121/251
Cross-Site Request Forgery (CSRF)	17-Dec-20	6.8	LogRhythm Platform Manager (PM) 7.4.9 allows CSRF. The Web interface is vulnerable to Cross-site WebSocket Hijacking (CSWH). If a logged-in PM user visits a malicious site in the same browser session, that site can perform a CSRF attack to create a WebSocket from the victim client to the vulnerable PM server. Once the socket is created, the malicious site can interact with the vulnerable web server in the context of the logged-in user. This can include WebSocket payloads that result in command execution. **CVE ID : CVE-2020-25095**	N/A	A-LOG-PLAT-040121/252
N/A	17-Dec-20	6.5	LogRhythm Platform Manager (PM) 7.4.9 has	N/A	A-LOG-PLAT-040121/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Incorrect Access Control. Users within LogRhythm can be delegated different roles and privileges, intended to limit what data and services they can interact with. However, no access control is enforced for WebSocket-based communication to the PM application server, which will forward requests to any configured back-end server, regardless of whether the user's access rights should permit this. As a result, even the most low-privileged user can interact with any back-end component that has a LogRhythm agent installed. **CVE ID : CVE-2020-25096**		
magic_home_pro_project					
magic_home_pro					
Improper Authentication	17-Dec-20	5	The Magic Home Pro application 1.5.1 for Android allows Authentication Bypass. The security control that the application currently has in place is a simple Username and Password authentication function. Using enumeration, an attacker is able to forge a User specific token without the need for correct password to gain access to the mobile application as	N/A	A-MAG-MAGI-040121/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that victim user. **CVE ID : CVE-2020-27199**		
Malwarebytes					
endpoint_protection					
Improper Link Resolution Before File Access ('Link Following')	22-Dec-20	6.6	In Malwarebytes Free 4.1.0.56, a symbolic link may be used delete an arbitrary file on the system by exploiting the local quarantine system. **CVE ID : CVE-2020-28641**	https://support.malwarebytes.com/hc/en-us/articles/1500000403501-Arbitrary-file-deletion-vulnerability-fixed-in-Malwarebytes-Endpoint-Protection	A-MAL-ENDP-040121/255
malwarebytes					
Improper Link Resolution Before File Access ('Link Following')	22-Dec-20	6.6	In Malwarebytes Free 4.1.0.56, a symbolic link may be used delete an arbitrary file on the system by exploiting the local quarantine system. **CVE ID : CVE-2020-28641**	https://support.malwarebytes.com/hc/en-us/articles/1500000403501-Arbitrary-file-deletion-vulnerability-fixed-in-Malwarebytes-Endpoint-Protection	A-MAL-MALW-040121/256
Mariadb					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mariadb					
N/A	24-Dec-20	4.4	With MariaDB running on Windows, when local clients connect to the server over named pipes, it's possible for an unprivileged user with an ability to run code on the server machine to intercept the named pipe connection and act as a man-in-the-middle, gaining access to all the data passed between the client and the server, and getting the ability to run SQL commands on behalf of the connected user. This occurs because of an incorrect security descriptor. This affects MariaDB Server before 10.1.48, 10.2.x before 10.2.35, 10.3.x before 10.3.26, 10.4.x before 10.4.16, and 10.5.x before 10.5.7. NOTE: this issue exists because certain details of the MariaDB CVE-2019-2503 fix did not comprehensively address attack variants against MariaDB. This situation is specific to MariaDB, and thus CVE-2020-28912 does NOT apply to other vendors that were originally affected by CVE-2019-2503. **CVE ID : CVE-2020-28912**	N/A	A-MAR-MARI-040121/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Marvell					
qconvergeconsole					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-20	8.5	Relative Path Traversal in Marvell QConvergeConsole GUI 5.5.0.74 allows a remote, authenticated attacker to delete arbitrary files on disk as SYSTEM or root. **CVE ID : CVE-2020-5803**	N/A	A-MAR-QCON-040121/258
Mediawiki					
mediawiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	In MediaWiki before 1.35.1, the combination of Html::rawElement and Message::text leads to XSS because the definition of MediaWiki:recentchanges-legend-watchlistexpiry can be changed onwiki so that the output is raw HTML. **CVE ID : CVE-2020-35474**	N/A	A-MED-MEDI-040121/259
Improper Encoding or Escaping of Output	18-Dec-20	5	In MediaWiki before 1.35.1, the messages userrights-expiry-current and userrights-expiry-none can contain raw HTML. XSS can happen when a user visits Special:UserRights but does not have rights to change all userrights, and the table on the left side has unchangeable groups in it. (The right column with the changeable groups is not affected and is escaped correctly.) **CVE ID : CVE-2020-35475**	N/A	A-MED-MEDI-040121/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Dec-20	5	MediaWiki before 1.35.1 blocks legitimate attempts to hide log entries in some situations. If one sets MediaWiki:Mainpage to Special:MyLanguage/Main Page, visits a log entry on Special:Log, and toggles the "Change visibility of selected log entries" checkbox (or a tags checkbox) next to it, there is a redirection to the main page's action=historysubmit (instead of the desired behavior in which a revision-deletion form appears). **CVE ID : CVE-2020-35477**	N/A	A-MED-MEDI-040121/261
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	MediaWiki before 1.35.1 allows XSS via BlockLogFormatter.php. MediaWiki:blanknamespace potentially can be output as raw HTML with SCRIPT tags via LogFormatter::makePageLink(). This affects MediaWiki 1.33.0 and later. **CVE ID : CVE-2020-35478**	N/A	A-MED-MEDI-040121/262
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	MediaWiki before 1.35.1 allows XSS via BlockLogFormatter.php. Language::translateBlockExpiry itself does not escape in all code paths. For example, the return of Language::userTimeAndDate is is always unsafe for	N/A	A-MED-MEDI-040121/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML in a month value. This affects MediaWiki 1.12.0 and later. **CVE ID : CVE-2020-35479**		
Information Exposure	18-Dec-20	5	An issue was discovered in MediaWiki before 1.35.1. Missing users (accounts that don't exist) and hidden users (accounts that have been explicitly hidden due to being abusive, or similar) that the viewer cannot see are handled differently, exposing sensitive information about the hidden status to unprivileged viewers. This exists on various code paths. **CVE ID : CVE-2020-35480**	N/A	A-MED-MEDI-040121/264
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-20	4.3	An issue was discovered in the GlobalUsage extension for MediaWiki through 1.35.1. SpecialGlobalUsage.php calls WikiMap::makeForeignLink unsafely. The $page variable within the formatItem function was not being properly escaped, allowing for XSS under certain conditions. **CVE ID : CVE-2020-35622**	N/A	A-MED-MEDI-040121/265
Insufficiently Protected Credentials	21-Dec-20	5	An issue was discovered in the CasAuth extension for MediaWiki through 1.35.1. Due to improper username	N/A	A-MED-MEDI-040121/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation, it allowed user impersonation with trivial manipulations of certain characters within a given username. An ordinary user may be able to login as a "bureaucrat user" who has a similar username, as demonstrated by usernames that differ only in (1) bidirectional override symbols or (2) blank space. **CVE ID : CVE-2020-35623**		
Information Exposure Through Discrepancy	21-Dec-20	5	An issue was discovered in the SecurePoll extension for MediaWiki through 1.35.1. The non-admin vote list contains a full vote timestamp, which may provide unintended clues about how a voting process unfolded. **CVE ID : CVE-2020-35624**	N/A	A-MED-MEDI-040121/267
Incorrect Permission Assignment for Critical Resource	21-Dec-20	6.5	An issue was discovered in the Widgets extension for MediaWiki through 1.35.1. Any user with the ability to edit pages within the Widgets namespace could call any static function within any class (defined within PHP or MediaWiki) via a crafted HTML comment, related to a Smarty template. For example, a person in the Widget Editors group could use \MediaWiki\Shell\Shell::co	N/A	A-MED-MEDI-040121/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mmand within a comment. **CVE ID : CVE-2020-35625**		
Cross-Site Request Forgery (CSRF)	21-Dec-20	6.8	An issue was discovered in the PushToWatch extension for MediaWiki through 1.35.1. The primary form did not implement an anti-CSRF token and therefore was completely vulnerable to CSRF attacks against onSkinAddFooterLinks in PushToWatch.php. **CVE ID : CVE-2020-35626**	N/A	A-MED-MEDI-040121/269
Microsoft					
azure_sphere					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-Dec-20	7.2	A code execution vulnerability exists in the normal world's signed code execution functionality of Microsoft Azure Sphere 20.07. A specially crafted AF_PACKET socket can cause a process to create an executable memory mapping with controllable content. An attacker can execute a shellcode that uses the PACKET_MMAP functionality to trigger this vulnerability. **CVE ID : CVE-2020-35608**	N/A	A-MIC-AZUR-040121/270
Improper Neutralization of Special Elements in Output Used by a Downstream	22-Dec-20	2.1	A denial-of-service vulnerability exists in the asynchronous ioctl functionality of Microsoft Azure Sphere 20.05. A sequence of specially	N/A	A-MIC-AZUR-040121/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			crafted ioctl calls can cause a denial of service. An attacker can write shellcode to trigger this vulnerability. **CVE ID : CVE-2020-35609**		
miniweb_http_server_project					
miniweb_http_server					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Dec-20	5	MiniWeb HTTP server 0.8.19 allows remote attackers to cause a denial of service (daemon crash) via a long name for the first parameter in a POST request. **CVE ID : CVE-2020-29596**	N/A	A-MIN-MINI-040121/272
Mitel					
businesscti_enterprise					
Improper Input Validation	18-Dec-20	6.5	The chat window of Mitel BusinessCTI Enterprise (MBC-E) Client for Windows before 6.4.11 and 7.x before 7.0.3 could allow an attacker to gain access to user information by sending arbitrary code, due to improper input validation. A successful exploit could allow an attacker to view the user information and application data. **CVE ID : CVE-2020-27154**	N/A	A-MIT-BUSI-040121/273
micontact_center_business					
N/A	18-Dec-20	2.1	The Ignite portal in Mitel MiContact Center Business before 9.3.0.0 could allow a	N/A	A-MIT-MICO-040121/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local attacker to view system information due to insufficient output sanitization. **CVE ID : CVE-2020-24693**		
micollab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	The AWV component of Mitel MiCollab before 9.2 could allow an attacker to view system information by sending arbitrary code due to improper input validation, aka XSS. **CVE ID : CVE-2020-25606**	N/A	A-MIT-MICO-040121/275
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-20	6.5	The SAS portal of Mitel MiCollab before 9.2 could allow an attacker to access user credentials due to improper input validation, aka SQL Injection. **CVE ID : CVE-2020-25608**	N/A	A-MIT-MICO-040121/276
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	3.5	The NuPoint Messenger Portal of Mitel MiCollab before 9.2 could allow an authenticated attacker to execute arbitrary scripts due to insufficient input validation, aka XSS. A successful exploit could allow an attacker to view and modify user data. **CVE ID : CVE-2020-25609**	N/A	A-MIT-MICO-040121/277
Incorrect Authorization	18-Dec-20	5	The AWV component of Mitel MiCollab before 9.2 could allow an attacker to gain access to a web conference due to	N/A	A-MIT-MICO-040121/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient access control for conference codes. **CVE ID : CVE-2020-25610**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	The AWV portal of Mitel MiCollab before 9.2 could allow an attacker to gain access to conference information by sending arbitrary code due to improper input validation, aka XSS. Successful exploitation could allow an attacker to view user conference information. **CVE ID : CVE-2020-25611**	N/A	A-MIT-MICO-040121/279
Incorrect Authorization	18-Dec-20	4	The NuPoint Messenger of Mitel MiCollab before 9.2 could allow an attacker with escalated privilege to access user files due to insufficient access control. Successful exploit could potentially allow an attacker to gain access to sensitive information. **CVE ID : CVE-2020-25612**	N/A	A-MIT-MICO-040121/280
URL Redirection to Untrusted Site ('Open Redirect')	18-Dec-20	5.8	The online help portal of Mitel MiCollab before 9.2 could allow an attacker to redirect a user to an unauthorized website by executing malicious script due to insufficient access control. **CVE ID : CVE-2020-27340**	N/A	A-MIT-MICO-040121/281
multi-ini_project					
multi-ini					
Uncontrolled	22-Dec-20	7.5	This affects the package	https://git	A-MUL-MULT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			multi-ini before 2.1.1. It is possible to pollute an object's prototype by specifying the proto object as part of an array. **CVE ID : CVE-2020-28448**	hub.com/evangelion1204/multi-ini/pull/37, https://snyk.io/vuln/SNYK-JS-MULTIINI-1048969	040121/282
Uncontrolled Resource Consumption	22-Dec-20	7.5	This affects the package multi-ini before 2.1.2. It is possible to pollute an object's prototype by specifying the constructor.proto object as part of an array. This is a bypass of CVE-2020-28448. **CVE ID : CVE-2020-28460**	https://github.com/evangelion1204/multi-ini/commit/6b2212b2ce152c19538a2431415f72942c5a1bde, https://snyk.io/vuln/SNYK-JS-MULTIINI-1053229	A-MUL-MULT-040121/283
Nagios					
nagios_core					
Cross-Site Request Forgery (CSRF)	23-Dec-20	6.8	There is a Cross Site Request Forgery (CSRF) vulnerability in Nagios Core 4.2.4. **CVE ID : CVE-2020-35269**	N/A	A-NAG-NAGI-040121/284
Nchsoftware					
express_accounts					
Cleartext Storage of Sensitive Information	28-Dec-20	2.1	NCH Express Accounts 8.24 and earlier allows local users to discover the cleartext password by reading the configuration	N/A	A-NCH-EXPR-040121/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file. **CVE ID : CVE-2020-13473**		
Improper Privilege Management	28-Dec-20	4	In NCH Express Accounts 8.24 and earlier, an authenticated low-privilege user can enter a crafted URL to access higher-privileged functionalities such as Add/Edit users. **CVE ID : CVE-2020-13474**	N/A	A-NCH-EXPR-040121/286
express_invoice					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Dec-20	3.5	NCH Express Invoice 8.06 to 8.24 is vulnerable to Reflected XSS in the Quotes List module. **CVE ID : CVE-2020-13476**	N/A	A-NCH-EXPR-040121/287
NEC					
ism_server					
Improper Certificate Validation	24-Dec-20	5.8	iSM client versions from V5.1 prior to V12.1 running on NEC Storage Manager or NEC Storage Manager Express does not verify a server certificate properly, which allows a man-in-the-middle attacker to eavesdrop on an encrypted communication or alter the communication via a crafted certificate. **CVE ID : CVE-2020-5684**	N/A	A-NEC-ISM_-040121/288
niftypm					
nifty-pm					
Improper	21-Dec-20	4.3	Nifty-PM CPE 2.3 is	N/A	A-NIF-NIFT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			affected by stored HTML injection. The impact is remote arbitrary code execution. **CVE ID : CVE-2020-26049**		040121/289
nopcommerce					
store					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Dec-20	3.5	nopCommerce Store 4.30 is affected by cross-site scripting (XSS) in the Schedule tasks name field. This vulnerability can allow an attacker to inject the XSS payload in Schedule tasks and each time any user will go to that page of the website, the XSS triggers and attacker can able to steal the cookie according to the crafted payload. **CVE ID : CVE-2020-29475**	N/A	A-NOP-STOR-040121/290
nzxt					
cam					
Information Exposure	18-Dec-20	2.1	An information disclosure vulnerability exists in the WinRing0x64 Driver Privileged I/O Read IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) Using the IRP 0x9c4060cc gives a low privilege user direct access to the IN instruction that is completely unrestrained at an elevated privilege level.	N/A	A-NZX-CAM-040121/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker can send a malicious IRP to trigger this vulnerability and this access could allow for information leakage of sensitive data. **CVE ID : CVE-2020-13509**		
Information Exposure	18-Dec-20	2.1	An information disclosure vulnerability exists in the WinRing0x64 Driver Privileged I/O Read IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) using the IRP 0x9c4060d0 gives a low privilege user direct access to the IN instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13510**	N/A	A-NZX-CAM-040121/292
Information Exposure	18-Dec-20	2.1	An information disclosure vulnerability exists in the WinRing0x64 Driver Privileged I/O Read IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) using the IRP 0x9c4060d4 gives a low privilege user direct access to the IN instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability.	N/A	A-NZX-CAM-040121/293

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13511		
Improper Privilege Management	18-Dec-20	7.2	A privilege escalation vulnerability exists in the WinRing0x64 Driver Privileged I/O Write IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. Using the IRP 0x9c40a0d8 gives a low privilege user direct access to the OUT instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13512**	N/A	A-NZX-CAM-040121/294
Improper Privilege Management	18-Dec-20	7.2	A privilege escalation vulnerability exists in the WinRing0x64 Driver Privileged I/O Write IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. Using the IRP 0x9c40a0dc gives a low privilege user direct access to the OUT instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13513**	N/A	A-NZX-CAM-040121/295
Improper Privilege	18-Dec-20	7.2	A privilege escalation vulnerability exists in the	N/A	A-NZX-CAM-040121/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			WinRing0x64 Driver Privileged I/O Write IRPs functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. Using the IRP 0x9c40a0e0 gives a low privilege user direct access to the OUT instruction that is completely unrestrained at an elevated privilege level. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13514**		
Improper Privilege Management	18-Dec-20	7.2	A privilege escalation vulnerability exists in the WinRing0x64 Driver IRP 0x9c40a148 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause an adversary to obtain elevated privileges. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13515**	N/A	A-NZX-CAM-040121/297
Information Exposure	18-Dec-20	2.1	An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c406144 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger	N/A	A-NZX-CAM-040121/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability. **CVE ID : CVE-2020-13516**		
Information Exposure	18-Dec-20	2.1	An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c406104 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13517**	N/A	A-NZX-CAM-040121/299
Information Exposure	18-Dec-20	2.1	An information disclosure vulnerability exists in the WinRing0x64 Driver IRP 0x9c402084 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13518**	N/A	A-NZX-CAM-040121/300
Improper Privilege Management	18-Dec-20	7.2	A privilege escalation vulnerability exists in the WinRing0x64 Driver IRP 0x9c402088 functionality of NZXT CAM 4.8.0. A specially crafted I/O request packet (IRP) can cause increased privileges. An attacker can send a malicious IRP to trigger this vulnerability.	N/A	A-NZX-CAM-040121/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13519		
Odoo					
odoo					
Improper Privilege Management	22-Dec-20	6.5	A sandboxing issue in Odoo Community 11.0 through 13.0 and Odoo Enterprise 11.0 through 13.0, when running with Python 3.6 or later, allows remote authenticated users to execute arbitrary code, leading to privilege escalation. **CVE ID : CVE-2020-29396**	N/A	A-ODO-ODOO-040121/302
online_health_care_system_project					
online_health_care_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Dec-20	7.5	SourceCodester Online Health Care System 1.0 is affected by SQL Injection which allows a potential attacker to bypass the authentication system and become an admin. **CVE ID : CVE-2020-28074**	N/A	A-ONL-ONLI-040121/303
online_marriage_registration_system_project					
online_marriage_registration_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-20	6.5	The Online Marriage Registration System 1.0 post parameter "searchdata" in the user/search.php request is vulnerable to Time Based Sql Injection. **CVE ID : CVE-2020-35151**	N/A	A-ONL-ONLI-040121/304
onstove					
stove					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Dec-20	6.8	A arbitrary code execution vulnerability exists in the way that the Stove client improperly validates input value. An attacker could execute arbitrary code when the user access to crafted web page. This issue affects: Smilegate STOVE Client 0.0.4.72. **CVE ID : CVE-2020-7838**	N/A	A-ONS-STOV-040121/305
Opencart					
opencart					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Dec-20	3.5	OpenCart 3.0.3.6 is affected by cross-site scripting (XSS) in the Subject field of mail. This vulnerability can allow an attacker to inject the XSS payload in the Subject field of the mail and each time any user will open that mail of the website, the XSS triggers and the attacker can able to steal the cookie according to the crafted payload. **CVE ID : CVE-2020-29470**	N/A	A-OPE-OPEN-040121/306
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Dec-20	3.5	OpenCart 3.0.3.6 is affected by cross-site scripting (XSS) in the Profile Image. An admin can upload a profile image as a malicious code using JavaScript. Whenever anyone will see the profile picture, the code will execute and XSS will trigger. **CVE ID : CVE-2020-29471**	N/A	A-OPE-OPEN-040121/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
opendkim					
opendkim					
Improper Link Resolution Before File Access ('Link Following')	28-Dec-20	4.4	The test suite in libopendkim in OpenDKIM through 2.10.3 allows local users to gain privileges via a symlink attack against the /tmp/testkeys file (related to t-testdata.h, t-setup.c, and t-cleanup.c). NOTE: this is applicable to persons who choose to engage in the "A number of self-test programs are included here for unit-testing the library" situation. **CVE ID : CVE-2020-35766**	N/A	A-OPE-OPEN-040121/308
openslides					
openslides					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	3.5	OpenSlides is a free, Web-based presentation and assembly system for managing and projecting agenda, motions, and elections of assemblies. OpenSlides version 3.2, due to unsufficient user input validation and escaping, it is vulnerable to persistant cross-site scripting (XSS). In the web applications users can enter rich text in various places, e.g. for personal notes or in motions. These fields can be used to store arbitrary JavaScript Code that will be executed when other users	https://github.com/OpenSlides/OpenSlides/security/advisories/GHSA-w5wr-98qm-jx92	A-OPE-OPEN-040121/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read the respective text. An attacker could utilize this vulnerability be used to manipulate votes of other users, hijack the moderators session or simply disturb the meeting. The vulnerability was introduced with 6eae497abeab234418dfbd9d299e831eff86ed45 on 16.04.2020, which is first included in the 3.2 release. It has been patched in version 3.3 (in commit f3809fc8a97ee305d721662a75f788f9e9d21938, merged in master on 20.11.2020). **CVE ID : CVE-2020-26280**		
opensmtpd					
opensmtpd					
Missing Release of Resource after Effective Lifetime	24-Dec-20	5	smtpd/table.c in OpenSMTPD before 6.8.0p1 lacks a certain regfree, which might allow attackers to trigger a "very significant" memory leak via messages to an instance that performs many regex lookups. **CVE ID : CVE-2020-35679**	N/A	A-OPE-OPEN-040121/310
NULL Pointer Dereference	24-Dec-20	5	smtpd/lka_filter.c in OpenSMTPD before 6.8.0p1, in certain configurations, allows remote attackers to cause a denial of service (NULL pointer dereference and	N/A	A-OPE-OPEN-040121/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			daemon crash) via a crafted pattern of client activity, because the filter state machine does not properly maintain the I/O channel between the SMTP engine and the filters layer. **CVE ID : CVE-2020-35680**		
opentsdb					
opentsdb					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-20	7.5	A remote code execution vulnerability occurs in OpenTSDB through 2.4.0 via command injection in the yrange parameter. The yrange value is written to a gnuplot file in the /tmp directory. This file is then executed via the mygnuplot.sh shell script. (tsd/GraphHandler.java attempted to prevent command injections by blocking backticks but this is insufficient.) **CVE ID : CVE-2020-35476**	N/A	A-OPE-OPEN-040121/312
openzaak					
open_zaak					
Origin Validation Error	18-Dec-20	4.3	Open Zaak is a modern, open-source data- and services-layer to enable zaakgericht werken, a Dutch approach to case management. In Open Zaak before version 1.3.3 the Cross-Origin-Resource-Sharing policy in Open Zaak is currently wide	https://github.com/open-zaak/open-zaak/security/advisories/GHSA-chhr-gxrg-64x7	A-OPE-OPEN-040121/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			open - every client is allowed. This allows evil.com to run scripts that perform AJAX calls to known Open Zaak installations, and the browser will not block these. This was intended to only apply to development machines running on localhost/127.0.0.1. Open Zaak 1.3.3 disables CORS by default, while it can be opted-in through environment variables. The vulnerability does not actually seem exploitable because: a) The session cookie has a `Same-Site: Lax` policy which prevents it from being sent along in Cross-Origin requests. b) All pages that give access to (production) data are login-protected c) `Access-Control-Allow-Credentials` is set to `false` d) CSRF checks probably block the remote origin, since they're not explicitly added to the trusted allowlist. **CVE ID : CVE-2020-26251**		
Opera					
opera					
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-Dec-20	4.3	URLs using "javascript:" have the protocol removed when pasted into the address bar to protect users from cross-site scripting (XSS) attacks, but	N/A	A-OPE-OPER-040121/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			in certain circumstances this removal was not performed. This could allow users to be socially engineered to run an XSS attack against themselves. This vulnerability affects Opera for Android versions below 61.0.3076.56532. **CVE ID : CVE-2020-6159**		
Oracle					
cloud_infrastructure_identity_and_access_management					
N/A	22-Dec-20	6.5	Vulnerability in the Oracle Cloud Infrastructure Identity and Access Management product of Oracle Cloud Services. Easily exploitable vulnerability allows high privileged attacker with network access to compromise Oracle Cloud Infrastructure Identity and Access Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Cloud Infrastructure Identity and Access Management accessible data as well as unauthorized read access to a subset of Oracle Cloud Infrastructure Identity and Access Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of	N/A	A-ORA-CLOU-040121/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Cloud Infrastructure Identity and Access Management. All affected customers were notified of CVE-2020-14874 by Oracle. CVSS 3.1 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2020-14874**		
Ovirt					
ovirt-engine					
Improper Access Control	21-Dec-20	4	A flaw was found in ovirt-engine 4.4.3 and earlier allowing an authenticated user to read other users' personal information, including name, email and public SSH key. **CVE ID : CVE-2020-35497**	N/A	A-OVI-OVIR-040121/316
p11-kit_project					
p11-kit					
Integer Overflow or Wraparound	16-Dec-20	5	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple integer overflows have been discovered in the array allocations in the p11-kit library and the p11-kit list command, where overflow checks are missing before calling realloc or calloc. **CVE ID : CVE-2020-29361**	N/A	A-P11-P11--040121/317
Out-of-bounds Read	16-Dec-20	6.4	An issue was discovered in p11-kit 0.21.1 through 0.23.21. A heap-based	N/A	A-P11-P11--040121/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer over-read has been discovered in the RPC protocol used by thep11-kit server/remote commands and the client library. When the remote entity supplies a byte array through a serialized PKCS#11 function call, the receiving entity may allow the reading of up to 4 bytes of memory past the heap allocation. **CVE ID : CVE-2020-29362**		
Out-of-bounds Write	16-Dec-20	7.5	An issue was discovered in p11-kit 0.23.6 through 0.23.21. A heap-based buffer overflow has been discovered in the RPC protocol used by p11-kit server/remote commands and the client library. When the remote entity supplies a serialized byte array in a CK_ATTRIBUTE, the receiving entity may not allocate sufficient length for the buffer to store the deserialized value. **CVE ID : CVE-2020-29363**	N/A	A-P11-P11--040121/319
Parallels					
remote_application_server					
Information Exposure	25-Dec-20	5	Parallels Remote Application Server (RAS) 18 allows remote attackers to discover an intranet IP address because submission of the login	N/A	A-PAR-REMO-040121/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			form (even with blank credentials) provides this address to the attacker's client for use as a "host" value. In other words, after an attacker's web browser sent a request to the login form, it would automatically send a second request to a RASHTML5Gateway/socket.io URI with something like "host":"192.168.###.###" in the POST data. **CVE ID : CVE-2020-35710**		
pengutronix					
rauc					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-20	7.1	The install.c module in the Pengutronix RAUC update client prior to version 1.5 has a Time-of-Check Time-of-Use vulnerability, where signature verification on an update file takes place before the file is reopened for installation. An attacker who can modify the update file just before it is reopened can install arbitrary code on the device. **CVE ID : CVE-2020-25860**	N/A	A-PEN-RAUC-040121/321
Phplist					
phplist					
Improper Neutralization of Special	25-Dec-20	6.5	phpList 3.5.9 allows SQL injection by admins who provide a crafted fourth	N/A	A-PHP-PHPL-040121/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			line of a file to the "Config - Import Administrators" page. **CVE ID : CVE-2020-35708**		
pi-hole					
pi-hole					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	The DNS query log in Pi-hole before 5.2.2 is vulnerable to stored XSS. An attacker with the ability to directly or indirectly query DNS with a malicious hostname can cause arbitrary JavaScript to execute when the Pi-hole administrator visits the Query Log or Long-term data Query Log page. **CVE ID : CVE-2020-35659**	https://discourse.pi-hole.net/t/pi-hole-core-web-v5-2-2-and-ftl-v5-3-3-released/41998	A-PI--PI-H-040121/323
Plone					
plone					
Missing Authentication for Critical Function	17-Dec-20	10	The official plone Docker images before version of 4.3.18-alpine (Alpine specific) contain a blank password for a root user. System using the plone docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35190**	N/A	A-PLO-PLON-040121/324
Pluck-cms					
pluck					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	16-Dec-20	6.5	A file upload restriction bypass vulnerability in Pluck CMS before 4.7.13 allows an admin privileged user to gain access in the host through the "manage files" functionality, which may result in remote code execution. **CVE ID : CVE-2020-29607**	N/A	A-PLU-PLUC-040121/325
polarisoffice					
polaris_ml_report					
Out-of-bounds Write	16-Dec-20	6.8	An issue was discovered in ML Report Program. There is a stack-based buffer overflow in function sub_41EAF0 at MLReportDeamon.exe. The function will call vsprintf without checking the length of strings in parameters given by attacker. And it finally leads to a stack-based buffer overflow via access to crafted web page. This issue affects: Infraware ML Report 2.19.312.0000. **CVE ID : CVE-2020-7837**	N/A	A-POL-POLA-040121/326
postsrsd_prject					
postsrsd					
Uncontrolled Resource Consumption	20-Dec-20	5	srs2.c in PostSRSd before 1.10 allows remote attackers to cause a denial of service (CPU consumption) via a long timestamp tag in an SRS address.	N/A	A-POS-POST-040121/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35573		
predefine_project					
predefine					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'predefine' versions 0.0.0 through 0.1.2 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28280**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28280	A-PRE-PRED-040121/328
projectworlds					
online_matrimonial_project					
Unrestricted Upload of File with Dangerous Type	23-Dec-20	6.5	Marital - Online Matrimonial Project In PHP version 1.0 suffers from an authenticated file upload vulnerability allowing remote attackers to gain remote code execution (RCE) on the Hosting web server via uploading a maliciously crafted PHP file. **CVE ID : CVE-2020-27397**	N/A	A-PRO-ONLI-040121/329
Pureftpd					
pure-ftpd					
Allocation of Resources Without Limits or Throttling	26-Dec-20	5	Pure-FTPd 1.0.48 allows remote attackers to prevent legitimate server use by making enough connections to exceed the connection limit. **CVE ID : CVE-2020-35359**	N/A	A-PUR-PURE-040121/330
Python					
python					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	22-Dec-20	6.5	A sandboxing issue in Odoo Community 11.0 through 13.0 and Odoo Enterprise 11.0 through 13.0, when running with Python 3.6 or later, allows remote authenticated users to execute arbitrary code, leading to privilege escalation. **CVE ID : CVE-2020-29396**	N/A	A-PYT-PYTH-040121/331
Qnap					
qes					
Use of Hard-coded Credentials	24-Dec-20	4	A hard-coded password vulnerability has been reported to affect earlier versions of QES. If exploited, this vulnerability could allow attackers to log in with a hard-coded password. QNAP has already fixed the issue in QES 2.1.1 Build 20200515 and later. **CVE ID : CVE-2020-2499**	N/A	A-QNA-QES-040121/332
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	3.5	If exploited, this stored cross-site scripting vulnerability could allow remote attackers to inject malicious code in File Station. QNAP has already fixed these issues in QES 2.1.1 Build 20201006 and later. **CVE ID : CVE-2020-2503**	N/A	A-QNA-QES-040121/333
Improper Limitation of a Pathname to a	24-Dec-20	5	If exploited, this absolute path traversal vulnerability could allow attackers to	N/A	A-QNA-QES-040121/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			traverse files in File Station. QNAP has already fixed these issues in QES 2.1.1 Build 20201006 and later. **CVE ID : CVE-2020-2504**		
Information Exposure Through an Error Message	24-Dec-20	2.1	If exploited, this vulnerability could allow attackers to gain sensitive information via generation of error messages. QNAP has already fixed these issues in QES 2.1.1 Build 20201006 and later. **CVE ID : CVE-2020-2505**	N/A	A-QNA-QES-040121/335
raysync					
raysync					
Improper Control of Generation of Code ('Code Injection')	23-Dec-20	9.3	A RCE vulnerability exists in Raysync below 3.3.3.8. An unauthenticated unauthorized attacker sending a specifically crafted request to override the specific file in server with malicious content can login as "admin", then to modify specific shell file to achieve remote code execution(RCE) on the hosting server. **CVE ID : CVE-2020-35370**	N/A	A-RAY-RAYS-040121/336
Redhat					
openstack_platform					
Insufficiently Protected Credentials	18-Dec-20	3.6	User credentials can be manipulated and stolen by Native CephFS consumers of OpenStack Manila, resulting in potential	N/A	A-RED-OPEN-040121/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege escalation. An Open Stack Manila user can request access to a share to an arbitrary cephx user, including existing users. The access key is retrieved via the interface drivers. Then, all users of the requesting OpenStack project can view the access key. This enables the attacker to target any resource that the user has access to. This can be done to even "admin" users, compromising the ceph administrator. This flaw affects Ceph versions prior to 14.2.16, 15.x prior to 15.2.8, and 16.x prior to 16.2.0. **CVE ID : CVE-2020-27781**		
ceph					
Insufficiently Protected Credentials	18-Dec-20	3.6	User credentials can be manipulated and stolen by Native CephFS consumers of OpenStack Manila, resulting in potential privilege escalation. An Open Stack Manila user can request access to a share to an arbitrary cephx user, including existing users. The access key is retrieved via the interface drivers. Then, all users of the requesting OpenStack project can view the access key. This enables the attacker to target any	N/A	A-RED-CEPH-040121/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resource that the user has access to. This can be done to even "admin" users, compromising the ceph administrator. This flaw affects Ceph versions prior to 14.2.16, 15.x prior to 15.2.8, and 16.x prior to 16.2.0. **CVE ID : CVE-2020-27781**		
openshift_container_platform					
Insufficiently Protected Credentials	18-Dec-20	3.6	User credentials can be manipulated and stolen by Native CephFS consumers of OpenStack Manila, resulting in potential privilege escalation. An Open Stack Manila user can request access to a share to an arbitrary cephx user, including existing users. The access key is retrieved via the interface drivers. Then, all users of the requesting OpenStack project can view the access key. This enables the attacker to target any resource that the user has access to. This can be done to even "admin" users, compromising the ceph administrator. This flaw affects Ceph versions prior to 14.2.16, 15.x prior to 15.2.8, and 16.x prior to 16.2.0. **CVE ID : CVE-2020-27781**	N/A	A-RED-OPEN-040121/339
Misinterpretati	21-Dec-20	10	A signature verification	N/A	A-RED-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input			vulnerability exists in crewjam/saml. This flaw allows an attacker to bypass SAML Authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-27846**		040121/340
virtualization					
Improper Access Control	21-Dec-20	4	A flaw was found in ovirt-engine 4.4.3 and earlier allowing an authenticated user to read other users' personal information, including name, email and public SSH key. **CVE ID : CVE-2020-35497**	N/A	A-RED-VIRT-040121/341
openshift_service_mesh					
Misinterpretati on of Input	21-Dec-20	10	A signature verification vulnerability exists in crewjam/saml. This flaw allows an attacker to bypass SAML Authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-27846**	N/A	A-RED-OPEN-040121/342
ceph_storage					
Insufficiently Protected Credentials	18-Dec-20	3.6	User credentials can be manipulated and stolen by Native CephFS consumers of OpenStack Manila, resulting in potential privilege escalation. An	N/A	A-RED-CEPH-040121/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Open Stack Manila user can request access to a share to an arbitrary cephx user, including existing users. The access key is retrieved via the interface drivers. Then, all users of the requesting OpenStack project can view the access key. This enables the attacker to target any resource that the user has access to. This can be done to even "admin" users, compromising the ceph administrator. This flaw affects Ceph versions prior to 14.2.16, 15.x prior to 15.2.8, and 16.x prior to 16.2.0. **CVE ID : CVE-2020-27781**		
redislabs					
redisgraph					
NULL Pointer Dereference	23-Dec-20	5	RedisGraph 2.x through 2.2.11 has a NULL Pointer Dereference that leads to a server crash because it mishandles an unquoted string, such as an alias that has not yet been introduced. **CVE ID : CVE-2020-35668**	N/A	A-RED-REDI-040121/344
Rocklobster					
contact_form_7					
Unrestricted Upload of File with Dangerous	17-Dec-20	10	The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File	N/A	A-ROC-CONT-040121/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			Upload and remote code execution because a filename may contain special characters. **CVE ID : CVE-2020-35489**		
rockoa					
xinhu					
N/A	26-Dec-20	5	rainrocka xinhu 2.1.9 allows remote attackers to obtain sensitive information via an index.php?a=gettotal request in which the ajaxbool value is manipulated to be true. **CVE ID : CVE-2020-35388**	N/A	A-ROC-XINH-040121/346
Rockwellautomation					
factorytalk_diagnostics					
Improper Handling of Exceptional Conditions	29-Dec-20	5	An unauthenticated remote attacker can send data to RsvcHost.exe listening on TCP port 5241 to add entries in the FactoryTalk Diagnostics event log. The attacker can specify long fields in the log entry, which can cause an unhandled exception in wcscpy_s() if a local user opens FactoryTalk Diagnostics Viewer (FTDiagViewer.exe) to view the log entry. Observed in FactoryTalk Diagnostics 6.11. All versions of FactoryTalk Diagnostics are affected. **CVE ID : CVE-2020-5807**	https://www.tenable.com/security/research/tra-2020-71	A-ROC-FACT-040121/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
factorytalk_linx					
Improper Handling of Exceptional Conditions	29-Dec-20	5	An attacker can craft and send an OpenNamespace message to port 4241 with valid session-id that triggers an unhandled exception in CFTLDManager::HandleRequest function in RnaDaSvr.dll, resulting in process termination. Observed in FactoryTalk Linx 6.11. All versions of FactoryTalk Linx are affected. **CVE ID : CVE-2020-5801**	https://www.tenable.com/security/research/tra-2020-71	A-ROC-FACT-040121/348
Improper Handling of Exceptional Conditions	29-Dec-20	5	An attacker-controlled memory allocation size can be passed to the C++ new operator in RnaDaSvr.dll by sending a specially crafted ConfigureItems message to TCP port 4241. This will cause an unhandled exception, resulting in termination of RSLinxNG.exe. Observed in FactoryTalk 6.11. All versions of FactoryTalk Linx are affected. **CVE ID : CVE-2020-5802**	https://www.tenable.com/security/research/tra-2020-71	A-ROC-FACT-040121/349
Allocation of Resources Without Limits or Throttling	29-Dec-20	2.1	An attacker-controlled memory allocation size can be passed to the C++ new operator in the CServerManager::HandleBrowseLoadIconStreamRequest in messaging.dll. This can be done by sending a	https://www.tenable.com/security/research/tra-2020-71	A-ROC-FACT-040121/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted message to 127.0.0.1:7153. Observed in FactoryTalk Linx 6.11. All versions of FactoryTalk Linx are affected. **CVE ID : CVE-2020-5806**		
Roundcube					
roundcube					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Dec-20	4.3	An XSS issue was discovered in Roundcube Webmail before 1.2.13, 1.3.x before 1.3.16, and 1.4.x before 1.4.10. The attacker can send a plain text e-mail message, with JavaScript in a link reference element that is mishandled by linkref_addindex in rcube_string_replacer.php. **CVE ID : CVE-2020-35730**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=978491, https://github.com/roundcube/roundcubemail/compare/1.4.9...1.4.10, https://github.com/roundcube/roundcubemail/releases/tag/1.2.13, https://github.com/roundcube/roundcubemail/releases/tag/1.3.16	A-ROU-ROUN-040121/351
rust-lang					
async-h1					
Inconsistent Interpretation	21-Dec-20	5.8	async-h1 is an asynchronous HTTP/1.1	https://github.com/ht	A-RUS-ASYN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of HTTP Requests ('HTTP Request Smuggling')			parser for Rust (crates.io). There is a request smuggling vulnerability in async-h1 before version 2.3.0. This vulnerability affects any webserver that uses async-h1 behind a reverse proxy, including all such Tide applications. If the server does not read the body of a request which is longer than some buffer length, async-h1 will attempt to read a subsequent request from the body content starting at that offset into the body. One way to exploit this vulnerability would be for an adversary to craft a request such that the body contains a request that would not be noticed by a reverse proxy, allowing it to forge forwarded/x-forwarded headers. If an application trusted the authenticity of these headers, it could be misled by the smuggled request. Another potential concern with this vulnerability is that if a reverse proxy is sending multiple http clients' requests along the same keep-alive connection, it would be possible for the smuggled request to specify a long content and capture another user's request in	tp-rs/async-h1/security/advisories/GHSA-4vr9-8cjf-vf9c	040121/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			its body. This content could be captured in a post request to an endpoint that allows the content to be subsequently retrieved by the adversary. This has been addressed in async-h1 2.3.0 and previous versions have been yanked. **CVE ID : CVE-2020-26281**		
saml_project					
saml					
Misinterpretation of Input	21-Dec-20	10	A signature verification vulnerability exists in crewjam/saml. This flaw allows an attacker to bypass SAML Authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-27846**	N/A	A-SAM-SAML-040121/353
seacms					
seacms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-20	7.5	SQL injection vulnerability in SeaCMS 10.1 (2020.02.08) via the id parameter in an edit action to admin_members_group.php. **CVE ID : CVE-2020-21378**	N/A	A-SEA-SEAC-040121/354
set-object-value_project					
set-object-value					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'set-object-	https://www.whitesou	A-SET-SET--040121/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			value' versions 0.0.0 through 0.0.5 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28281**	rcesoftware.com/vulnerability-database/CVE-2020-28281	
shvl_project					
shvl					
N/A	29-Dec-20	7.5	Prototype pollution vulnerability in 'shvl' versions 1.0.0 through 2.0.1 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2020-28278**	https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28278	A-SHV-SHVL-040121/356
softwareag					
terracotta_server_oss					
Missing Authentication for Critical Function	16-Dec-20	10	The Software AG Terracotta Server OSS Docker image 5.4.1 contains a blank password for the root user. Systems deployed using affected versions of the Terracotta Server OSS container may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35469**	N/A	A-SOF-TERR-040121/357
Solarwinds					
n-central					
Improper Limitation of a Pathname to a Restricted Directory	16-Dec-20	9	An issue was discovered in SolarWinds N-Central 12.3.0.670. The AdvancedScripts HTTP endpoint allows Relative	N/A	A-SOL-N-CE-040121/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Path Traversal by an authenticated user of the N-Central Administration Console (NAC), leading to execution of OS commands as root. **CVE ID : CVE-2020-25617**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Dec-20	9	An issue was discovered in SolarWinds N-Central 12.3.0.670. The sudo configuration has incorrect access control because the nable web user account is effectively able to run arbitrary OS commands as root (i.e., the use of root privileges is not limited to specific programs listed in the sudoers file). **CVE ID : CVE-2020-25618**	N/A	A-SOL-N-CE-040121/359
N/A	16-Dec-20	3.6	An issue was discovered in SolarWinds N-Central 12.3.0.670. The SSH component does not restrict the Communication Channel to Intended Endpoints. An attacker can leverage an SSH feature (port forwarding with a temporary key pair) to access network services on the 127.0.0.1 interface, even though this feature was only intended for user-to-agent communication. **CVE ID : CVE-2020-25619**	N/A	A-SOL-N-CE-040121/360
Use of Hard-coded Credentials	16-Dec-20	4.6	An issue was discovered in SolarWinds N-Central 12.3.0.670. Hard-coded	N/A	A-SOL-N-CE-040121/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Credentials exist by default for local user accounts named support@n-able.com and nableadmin@n-able.com. These allow logins to the N-Central Administrative Console (NAC) and/or the regular web interface. **CVE ID : CVE-2020-25620**		
Improper Authentication	16-Dec-20	2.1	An issue was discovered in SolarWinds N-Central 12.3.0.670. The local database does not require authentication: security is only based on ability to access a network interface. The database has keys and passwords. **CVE ID : CVE-2020-25621**	N/A	A-SOL-N-CE-040121/362
Cross-Site Request Forgery (CSRF)	16-Dec-20	6.8	An issue was discovered in SolarWinds N-Central 12.3.0.670. The AdvancedScripts HTTP endpoint allows CSRF. **CVE ID : CVE-2020-25622**	N/A	A-SOL-N-CE-040121/363
orion_platform					
Improper Authentication	29-Dec-20	7.5	The SolarWinds Orion API is vulnerable to an authentication bypass that could allow a remote attacker to execute API commands. This vulnerability could allow a remote attacker to bypass authentication and execute API commands which may result in a compromise of the SolarWinds instance.	https://www.solarwinds.com/securityadvisory	A-SOL-ORIO-040121/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SolarWinds Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1 are affected. **CVE ID : CVE-2020-10148**		
Sonarsource					
sonarqube_docker_image					
Missing Authentication for Critical Function	16-Dec-20	10	The official sonarqube docker images before alpine (Alpine specific) contain a blank password for a root user. System using the sonarqube docker container deployed by affected versions of the docker image may allow a remote attacker to achieve root access with a blank password. **CVE ID : CVE-2020-35193**	N/A	A-SON-SONA-040121/365
Sonatype					
nexus_repository_manager					
Improper Restriction of XML External Entity Reference ('XXE')	17-Dec-20	5.5	Sonatype Nexus Repository Manager 3.x before 3.29.0 allows a user with admin privileges to configure the system to gain access to content outside of NXRM via an XXE vulnerability. Fixed in version 3.29.0. **CVE ID : CVE-2020-29436**	https://support.sonatype.com/hc/en-us/articles/1500000415082-CVE-2020-29436-Nexus-Repository-Manager-3-XML-External-Entities-	A-SON-NEXU-040121/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				injection-2020-12-15	
Spamtitan					
spamtitan					
Missing Encryption of Sensitive Data	23-Dec-20	5	SpamTitan before 7.09 allows attackers to tamper with backups, because backups are not encrypted. **CVE ID : CVE-2020-35658**	N/A	A-SPA-SPAM-040121/367
Spiceworks					
spiceworks					
URL Redirection to Untrusted Site ('Open Redirect')	18-Dec-20	5.8	Host Header Injection in Spiceworks 7.5.7.0 allowing the attacker to render arbitrary links that point to a malicious website with poisoned Host header webpages. **CVE ID : CVE-2020-25901**	N/A	A-SPI-SPIC-040121/368
spotweb_project					
spotweb					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Dec-20	7.5	Time-based SQL injection exists in Spotweb 1.4.9 via the query string. **CVE ID : CVE-2020-35545**	N/A	A-SPO-SPOT-040121/369
steedos					
steedos					
Improper Neutralization of Special Elements used in an SQL	23-Dec-20	6.5	Steedos Platform through 1.21.24 allows NoSQL injection because the /api/collection/findone implementation in	N/A	A-STE-STEE-040121/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			server/packages/steedos_base.js mishandles req.body validation, as demonstrated by MongoDB operator attacks such as an X-User-Id[$ne]=1 value. **CVE ID : CVE-2020-35666**		
stepmania					
stepmania					
Improper Validation of Array Index	26-Dec-20	4.3	lib/codebook.c in libvorbis before 1.3.6, as used in StepMania 5.0.12 and other products, has insufficient array bounds checking via a crafted OGG file. **CVE ID : CVE-2020-20412**	N/A	A-STE-STEP-040121/371
stratodesk					
notouch_center					
Improper Privilege Management	26-Dec-20	6.5	Stratodesk NoTouch Center before 4.4.68 is affected by: Incorrect Access Control. A low privileged user on the platform, for example a user with "helpdesk" privileges, can perform privileged operations including adding a new administrator to the platform via the easyadmin/user/submitCreateTCUser.do page. **CVE ID : CVE-2020-25917**	N/A	A-STR-NOTO-040121/372
struct2json_project					
struct2json					
Buffer Copy without Checking Size	26-Dec-20	7.5	struct2json before 2020-11-18 is affected by a Buffer Overflow because	N/A	A-STR-STRU-040121/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			strcpy is used for S2J_STRUCT_GET_string_ELEMENT. **CVE ID : CVE-2020-29203**		
subconverter_project					
subconverter					
N/A	20-Dec-20	5	tindy2013 subconverter 0.6.4 has a /sub?target=%TARGET%&url=%URL%&config=%CONFIG% API endpoint that accepts an arbitrary %URL% value and launches a GET request for it, but does not consider that the external request target may indirectly redirect back to this original /sub endpoint. Thus, a request loop and a denial of service may occur. **CVE ID : CVE-2020-35579**	N/A	A-SUB-SUBC-040121/374
supremocontrol					
supremo					
Unrestricted Upload of File with Dangerous Type	22-Dec-20	9.3	Nanosystems SupRemo 4.1.3.2348 allows attackers to obtain LocalSystem access because File Manager can be used to rename Supremo.exe and then upload a Trojan horse with the Supremo.exe filename. **CVE ID : CVE-2020-25106**	N/A	A-SUP-SUPR-040121/375
systeminformation					
systeminformation					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Dec-20	7.5	In systeminformation (npm package) before version 4.31.1 there is a command injection vulnerability. The problem was fixed in version 4.31.1 with a shell string sanitation fix. **CVE ID : CVE-2020-26274**	https://github.com/sebhildebrandt/systeminformation/security/advisories/GHSA-m57p-p67h-mq74	A-SYS-SYST-040121/376
tag_project					
tag					
Improper Validation of Array Index	28-Dec-20	4.3	dhowden tag before 2020-11-19 allows "panic: runtime error: index out of range" via readPICFrame. **CVE ID : CVE-2020-29242**	N/A	A-TAG-TAG-040121/377
Improper Validation of Array Index	28-Dec-20	4.3	dhowden tag before 2020-11-19 allows "panic: runtime error: index out of range" via readAPICFrame. **CVE ID : CVE-2020-29243**	N/A	A-TAG-TAG-040121/378
Improper Validation of Array Index	28-Dec-20	4.3	dhowden tag before 2020-11-19 allows "panic: runtime error: slice bounds out of range" via readTextWithDescrFrame. **CVE ID : CVE-2020-29244**	N/A	A-TAG-TAG-040121/379
Improper Validation of Array Index	28-Dec-20	4.3	dhowden tag before 2020-11-19 allows "panic: runtime error: slice bounds out of range" via readAtomData. **CVE ID : CVE-2020-29245**	N/A	A-TAG-TAG-040121/380
tangro					
business_workflow					
Incorrect Permission	18-Dec-20	4	In tangro Business Workflow before 1.18.1,	N/A	A-TAN-BUSI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			the documentId of attachment uploads to /api/document/attachments/upload can be manipulated. By doing this, users can add attachments to workitems that do not belong to them. **CVE ID : CVE-2020-26171**		040121/381
Authentication Bypass by Capture-replay	18-Dec-20	6.4	Every login in tangro Business Workflow before 1.18.1 generates the same JWT token, which allows an attacker to reuse the token when a session is active. The JWT token does not contain an expiration timestamp. **CVE ID : CVE-2020-26172**	N/A	A-TAN-BUSI-040121/382
Improper Authentication	18-Dec-20	4	An incorrect access control implementation in Tangro Business Workflow before 1.18.1 allows an attacker to download documents (PDF) by providing a valid document ID and token. No further authentication is required. **CVE ID : CVE-2020-26173**	N/A	A-TAN-BUSI-040121/383
Unrestricted Upload of File with Dangerous Type	18-Dec-20	6.5	tangro Business Workflow before 1.18.1 requests a list of allowed filetypes from the server and restricts uploads to the filetypes contained in this list. However, this restriction is enforced in the browser (client-side) and can be circumvented. This allows	N/A	A-TAN-BUSI-040121/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker to upload any file as an attachment to a workitem. **CVE ID : CVE-2020-26174**		
Incorrect Permission Assignment for Critical Resource	18-Dec-20	4	In tangro Business Workflow before 1.18.1, an attacker can manipulate the value of PERSON in requests to /api/profile in order to change profile information of other users. **CVE ID : CVE-2020-26175**	N/A	A-TAN-BUSI-040121/385
Insecure Storage of Sensitive Information	18-Dec-20	4	An issue was discovered in tangro Business Workflow before 1.18.1. No (or broken) access control checks exist on the /api/document/<DocumentID>/attachments API endpoint. Knowing a document ID, an attacker can list all the attachments of a workitem, including their respective IDs. This allows the attacker to gather valid attachment IDs for workitems that do not belong to them. **CVE ID : CVE-2020-26176**	N/A	A-TAN-BUSI-040121/386
Incorrect Permission Assignment for Critical Resource	18-Dec-20	4	In tangro Business Workflow before 1.18.1, a user's profile contains some items that are greyed out and thus are not intended to be edited by regular users. However, this restriction is only applied client-side. Manipulating any of the	N/A	A-TAN-BUSI-040121/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			greyed-out values in requests to /api/profile is not prohibited server-side. **CVE ID : CVE-2020-26177**		
Authorization Bypass Through User-Controlled Key	18-Dec-20	5	In tangro Business Workflow before 1.18.1, knowing an attachment ID, it is possible to download workitem attachments without being authenticated. **CVE ID : CVE-2020-26178**	N/A	A-TAN-BUSI-040121/388
td-agent-builder_project					
td-agent-builder					
Incorrect Permission Assignment for Critical Resource	24-Dec-20	6.9	The td-agent-builder plugin before 2020-12-18 for Fluentd allows attackers to gain privileges because the bin directory is writable by a user account, but a file in bin is executed as NT AUTHORITY\SYSTEM. **CVE ID : CVE-2020-28169**	https://github.com/fluent/fluentd/issues/3201, https://github.com/fluent-plugins-nursery/td-agent-builder/pull/247/commits/6f9cb6393392d62caa99907c0ebbcbab6b94a3f1, https://github.com/kenhys/td-agent-builder/commit/eec6e2dedf12f2	A-TD--TD-A-040121/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				e0c01c2bbe7b8c15b639b3b938	
techkshetrainfo					
savsoft_quiz					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Dec-20	4.3	A Cross Site Scripting (XSS) vulnerability in Savsoft Quiz v5.0 allows remote attackers to inject arbitrary web script or HTML via the Skype ID field. **CVE ID : CVE-2020-27515**	N/A	A-TEC-SAVS-040121/390
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Dec-20	3.5	Savsoft Quiz 5 is affected by: Cross Site Scripting (XSS) via field_title (aka a title on the custom fields page). **CVE ID : CVE-2020-35349**	N/A	A-TEC-SAVS-040121/391
Tenable					
tenable.sc					
Incorrect Permission Assignment for Critical Resource	21-Dec-20	5	In certain scenarios in Tenable.sc prior to 5.17.0, a scanner could potentially be used outside the user's defined scan zone without a particular zone being specified within the Automatic Distribution configuration. **CVE ID : CVE-2020-5808**	N/A	A-TEN-TENA-040121/392
tengine_project					
tengine					
Buffer Copy without Checking Size of Input	26-Dec-20	4.3	** DISPUTED ** The serializer module in OAID Tengine lite-v1.0 has a Buffer Overflow and crash.	N/A	A-TEN-TENG-040121/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			NOTE: another person has stated "I don't think there is an proof of overflow so far." **CVE ID : CVE-2020-28759**		
thingsboard					
thingsboard					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Dec-20	6.8	ThingsBoard before v3.2 is vulnerable to Host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails to victims, pointing to an attacker-controlled server. Lack of validation of the Host header allows this to happen. **CVE ID : CVE-2020-27687**	N/A	A-THI-THIN-040121/394
tlslite-ng_project					
tlslite-ng					
Inadequate Encryption Strength	21-Dec-20	5	tlslite-ng is an open source python library that implements SSL and TLS cryptographic protocols. In tlslite-ng before versions 0.7.6 and 0.8.0-alpha39, the code that performs decryption and padding check in RSA PKCS#1 v1.5 decryption is data dependant. In particular, the code has multiple ways in which it leaks information about the decrypted ciphertext. It aborts as soon as the plaintext doesn't start with	https://github.com/tlsfuzzer/tlslite-ng/security/advisories/GHSA-wvcv-832q-fjg7	A-TLS-TLSL-040121/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0x00, 0x02. All TLS servers that enable RSA key exchange as well as applications that use the RSA decryption API directly are vulnerable. This is patched in versions 0.7.6 and 0.8.0-alpha39. Note: the patches depend on Python processing the individual bytes in side-channel free manner, this is known to not the case (see reference). As such, users that require side-channel resistance are recommended to use different TLS implementations, as stated in the security policy of tlslite-ng. **CVE ID : CVE-2020-26263**		
treck					
tcp\/ip					
Out-of-bounds Write	22-Dec-20	7.5	A heap-based buffer overflow in the Treck HTTP Server component before 6.0.1.68 allows remote attackers to cause a denial of service (crash/reset) or to possibly execute arbitrary code. **CVE ID : CVE-2020-25066**	https://treck.com/vulnerability-response-information/	A-TRE-TCP\-040121/396
ipv6					
Out-of-bounds Read	22-Dec-20	5	An issue was discovered in Treck IPv6 before 6.0.1.68. Improper input validation in the IPv6 component when handling a packet	https://treck.com/vulnerability-response-informatio	A-TRE-IPV6-040121/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sent by an unauthenticated remote attacker could result in an out-of-bounds read of up to three bytes via network access. **CVE ID : CVE-2020-27336**	n/	
Out-of-bounds Write	22-Dec-20	7.5	An issue was discovered in Treck IPv6 before 6.0.1.68. Improper Input Validation in the IPv6 component allows an unauthenticated remote attacker to cause an Out of Bounds Write, and possibly a Denial of Service via network access. **CVE ID : CVE-2020-27337**	https://treck.com/vulnerability-response-information/	A-TRE-IPV6-040121/398
Out-of-bounds Read	22-Dec-20	4.8	An issue was discovered in Treck IPv6 before 6.0.1.68. Improper Input Validation in the DHCPv6 client component allows an unauthenticated remote attacker to cause an Out of Bounds Read, and possibly a Denial of Service via adjacent network access. **CVE ID : CVE-2020-27338**	https://treck.com/vulnerability-response-information/	A-TRE-IPV6-040121/399
Trendmicro					
interscan_web_security_virtual_appliance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	3.5	A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to tamper with the web interface of the product in a manner separate from the similar	N/A	A-TRE-INTE-040121/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-8462. **CVE ID : CVE-2020-27010**		
Cross-Site Request Forgery (CSRF)	17-Dec-20	6.8	A CSRF protection bypass vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to get a victim's browser to send a specifically encoded request without requiring a valid CSRF token. **CVE ID : CVE-2020-8461**	N/A	A-TRE-INTE-040121/401
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	3.5	A cross-site scripting (XSS) vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to tamper with the web interface of the product. **CVE ID : CVE-2020-8462**	N/A	A-TRE-INTE-040121/402
Incorrect Authorization	17-Dec-20	5	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to bypass a global authorization check for anonymous users by manipulating request paths. **CVE ID : CVE-2020-8463**	N/A	A-TRE-INTE-040121/403
Server-Side Request Forgery (SSRF)	17-Dec-20	5	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to send requests that appear to come from the localhost which could	N/A	A-TRE-INTE-040121/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			expose the product's admin interface to users who would not normally have access. **CVE ID : CVE-2020-8464**		
Improper Authentication	17-Dec-20	10	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an attacker to manipulate system updates using a combination of CSRF bypass (CVE-2020-8461) and authentication bypass (CVE-2020-8464) to execute code as user root. **CVE ID : CVE-2020-8465**	N/A	A-TRE-INTE-040121/405
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Dec-20	7.5	A command injection vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2, with the improved password hashing method enabled, could allow an unauthenticated attacker to execute certain commands by providing a manipulated password. **CVE ID : CVE-2020-8466**	N/A	A-TRE-INTE-040121/406
Troglobit					
uftpd					
Out-of-bounds Write	18-Dec-20	7.5	An unauthenticated stack-based buffer overflow vulnerability in common.c's handle_PORT in uftpd FTP server versions 2.10 and earlier can be abused to cause a	N/A	A-TRO-UFTP-040121/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash and could potentially lead to remote code execution. **CVE ID : CVE-2020-20276**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-20	7.5	There are multiple unauthenticated directory traversal vulnerabilities in different FTP commands in uftpd FTP server versions 2.7 to 2.10 due to improper implementation of a chroot jail in common.c's compose_abspath function that can be abused to read or write to arbitrary files on the filesystem, leak process memory, or potentially lead to remote code execution. **CVE ID : CVE-2020-20277**	N/A	A-TRO-UFTP-040121/408
Twitter					
twitter-server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Dec-20	4.3	server/handler/HistogramQueryHandler.scala in Twitter TwitterServer (aka twitter-server) before 20.12.0, in some configurations, allows XSS via the /histograms endpoint. **CVE ID : CVE-2020-35774**	N/A	A-TWI-TWIT-040121/409
uncannyowl					
tin_canny_reporting_for_learndash					
Improper Neutralization of Input During Web Page Generation	23-Dec-20	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Uncanny Owl Tin Canny LearnDash Reporting before 3.4.4	N/A	A-UNC-TIN_-040121/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			allows authenticated remote attackers to inject arbitrary web script or HTML via the search_key GET Parameter in TinCan_Content_List_Table.php, message GET Parameter in licensing.php, tc_filter_group parameter in reporting-admin-menu.php, tc_filter_user parameter in reporting-admin-menu.php, tc_filter_course parameter in reporting-admin-menu.php, tc_filter_lesson parameter in reporting-admin-menu.php, tc_filter_module parameter in reporting-admin-menu.php, tc_filter_action parameter in reporting-admin-menu.php, tc_filter_data_range parameter in reporting-admin-menu.php, or tc_filter_data_range_last parameter in reporting-admin-menu.php. **CVE ID : CVE-2020-9439**		
uncanny_groups_for_learndash					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-20	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Uncanny Groups for LearnDash before v3.7 allow authenticated remote attackers to inject arbitrary JavaScript or HTML via the ulgm_code_redeem POST	N/A	A-UNC-UNCA-040121/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Parameter in user-code-redemption.php, the ulgm_user_first POST Parameter in user-registration-form.php, the ulgm_user_last POST Parameter in user-registration-form.php, the ulgm_user_email POST Parameter in user-registration-form.php, the ulgm_code_registration POST Parameter in user-registration-form.php, the ulgm_terms_conditions POST Parameter in user-registration-form.php, the _ulgm_total_seats POST Parameter in frontend-uo_groups_buy_courses.php, the uncanny_group_signup_user_first POST Parameter in group-registration-form.php, the uncanny_group_signup_user_last POST Parameter in group-registration-form.php, the uncanny_group_signup_user_login POST Parameter in group-registration-form.php, the uncanny_group_signup_user_email POST Parameter in group-registration-form.php, the success-invited GET Parameter in frontend-uo_groups.php, the bulk-errors GET Parameter in frontend-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uo_groups.php, or the message GET Parameter in frontend-uo_groups.php. **CVE ID : CVE-2020-35650**		
urve					
urve					
Cleartext Storage of Sensitive Information	23-Dec-20	5	An issue was discovered in URVE Build 24.03.2020. The password of an integration user account (used for the connection of the MS Office 365 Integration Service) is stored in cleartext in configuration files as well as in the database. The following files contain the password in cleartext: Profiles/urve/files/sql_db.backup, Server/data/pg_wal/0000 00010000000A000000DD, Server/data/base/16384/18617, and Server/data/base/17202/8708746. This causes the password to be displayed as cleartext in the HTML code as roomsreservationimport_password in /urve/roomsreservationimport/roomsreservationimport/update-HTML5. **CVE ID : CVE-2020-29550**	N/A	A-URV-URVE-040121/412
Missing Authorization	23-Dec-20	8.5	An issue was discovered in URVE Build 24.03.2020. Using the _internal/pc/shutdown.ph	N/A	A-URV-URVE-040121/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			p path, it is possible to shutdown the system. Among others, the following files and scripts are also accessible: _internal/pc/abort.php, _internal/pc/restart.php, _internal/pc/vpro.php, _internal/pc/wake.php, _internal/error_u201409.txt, _internal/runcmd.php, _internal/getConfiguration.php, ews/autoload.php, ews/del.php, ews/mod.php, ews/sync.php, utils/backup/backup_server.php, utils/backup/restore_server.php, MyScreens/timeline.config, kreator.html5/test.php, and addedlogs.txt. **CVE ID : CVE-2020-29551**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Dec-20	10	An issue was discovered in URVE Build 24.03.2020. By using the _internal/pc/vpro.php?mac=0&ip=0&operation=0&usr=0&pass=0%3bpowershell+-c+" substring, it is possible to execute a Powershell command and redirect its output to a file under the web root. **CVE ID : CVE-2020-29552**	N/A	A-URV-URVE-040121/414
user_registration_\&_login_and_user_management_system_with_admin_panel_project					
user_registration_\&_login_and_user_management_system_with_admin_panel					
Cross-Site	26-Dec-20	6.8	A Cross Site Request	N/A	A-USE-USER-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			Forgery (CSRF) vulnerability exists in the loginsystem page in PHPGurukul User Registration & Login and User Management System With Admin Panel 2.1. **CVE ID : CVE-2020-26766**		040121/415
Vmware					
workstation					
NULL Pointer Dereference	21-Dec-20	2.1	VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition. **CVE ID : CVE-2020-3999**	N/A	A-VMW-WORK-040121/416
fusion					
NULL Pointer Dereference	21-Dec-20	2.1	VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service	N/A	A-VMW-FUSI-040121/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition. **CVE ID : CVE-2020-3999**		
carbon_black_cloud					
N/A	16-Dec-20	3.6	The installer of the macOS Sensor for VMware Carbon Black Cloud prior to 3.5.1 handles certain files in an insecure way. A malicious actor who has local access to the endpoint on which a macOS sensor is going to be installed, may overwrite a limited number of files with output from the sensor installation. **CVE ID : CVE-2020-4008**	N/A	A-VMW-CARB-040121/418
Wavpack					
Wavpack					
Out-of-bounds Write	28-Dec-20	4.3	WavPack 5.3.0 has an out-of-bounds write in WavpackPackSamples in pack_utils.c because of an integer overflow in a malloc argument. NOTE: some third-parties claim that there are later "unofficial" releases through 5.3.2, which are also affected. **CVE ID : CVE-2020-35738**	N/A	A-WAV-WAVP-040121/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Webmin					
webmin					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Dec-20	9	Arbitrary command execution can occur in Webmin through 1.962. Any user authorized for the Package Updates module can execute arbitrary commands with root privileges via vectors involving %0A and %0C. NOTE: this issue exists because of an incomplete fix for CVE-2019-12840. **CVE ID : CVE-2020-35606**	N/A	A-WEB-WEBM-040121/420
N/A	29-Dec-20	7.5	miniserv.pl in Webmin 1.962 on Windows mishandles special characters in query arguments to the CGI program. **CVE ID : CVE-2020-35769**	N/A	A-WEB-WEBM-040121/421
weiphp					
weiphp					
Information Exposure	18-Dec-20	5	WeiPHP 5.0 does not properly restrict access to pages, related to using POST. **CVE ID : CVE-2020-20299**	N/A	A-WEI-WEIP-040121/422
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-20	7.5	SQL injection vulnerability in the wp_where function in WeiPHP 5.0. **CVE ID : CVE-2020-20300**	N/A	A-WEI-WEIP-040121/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
weseek					
growi					
Improper Input Validation	16-Dec-20	5	Improper input validation in GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier allows remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5682**	N/A	A-WES-GROW-040121/424
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Dec-20	5	Directory traversal vulnerability in GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier GROWI versions prior to v4.2.3 (v4.2 Series), GROWI versions prior to v4.1.12 (v4.1 Series), and GROWI v3 series and earlier allows remote attackers to alter the data by uploading a specially crafted file. **CVE ID : CVE-2020-5683**	N/A	A-WES-GROW-040121/425
Wireshark					
wireshark					
Buffer Copy without Checking Size	21-Dec-20	5	Buffer overflow in QUIC dissector in Wireshark 3.4.0 to 3.4.1 allows denial	https://gitlab.com/gitlab-	A-WIR-WIRE-040121/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			of service via packet injection or crafted capture file **CVE ID : CVE-2020-26422**	org/cves/-/blob/master/2020/CVE-2020-26422.json	
Wondercms					
wondercms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	4.3	WonderCMS 3.1.3 is affected by cross-site scripting (XSS) in the Admin Panel. An attacker can inject the XSS payload in Page keywords and each time any user will visit the website, the XSS triggers, and the attacker can able to steal the cookie according to the crafted payload. **CVE ID : CVE-2020-29247**	N/A	A-WON-WOND-040121/427
Woocommerce					
woocommerce					
Incorrect Authorization	27-Dec-20	5	The WooCommerce plugin before 4.7.0 for WordPress allows remote attackers to view the status of arbitrary orders via the order_id parameter in a fetch_order_status action. **CVE ID : CVE-2020-29156**	N/A	A-WOO-WOOC-040121/428
gift_cards					
Unrestricted Upload of File with Dangerous Type	28-Dec-20	7.5	Ultimate WooCommerce Gift Cards 3.0.2 is affected by a file upload vulnerability in the Custom GiftCard Template that can remotely execute arbitrary code. Once it contains the function "Custom Gift Card	N/A	A-WOO-GIFT-040121/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Template", the function of uploading a custom image is used, changing the name of the image extension to PHP and executing PHP code on the server. **CVE ID : CVE-2020-35627**		
Xinuos					
openserver					
Argument Injection or Modification	18-Dec-20	7.5	Xinuos (formerly SCO) Openserver v5 and v6 allows attackers to execute arbitrary commands via shell metacharacters in outputform or toclevels parameter to cgi-bin/printbook. **CVE ID : CVE-2020-25494**	N/A	A-XIN-OPEN-040121/430
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	A reflected Cross-site scripting (XSS) vulnerability in Xinuo (formerly SCO) Openserver version 5 and 6 allows remote attackers to inject arbitrary web script or HTML tag via the parameter 'section'. **CVE ID : CVE-2020-25495**	N/A	A-XIN-OPEN-040121/431
Xiph.org					
libvorbis					
Improper Validation of Array Index	26-Dec-20	4.3	lib/codebook.c in libvorbis before 1.3.6, as used in StepMania 5.0.12 and other products, has insufficient array bounds checking via a crafted OGG file. **CVE ID : CVE-2020-20412**	N/A	A-XIP-LIBV-040121/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xpdfreader					
xpdf					
Out-of-bounds Write	26-Dec-20	5	Xpdf 4.02 allows stack consumption because of an incorrect subroutine reference in a Type 1C font charstring, related to the FoFiType1C::getOp() function. **CVE ID : CVE-2020-35376**	N/A	A-XPD-XPDF-040121/433
xstream_project					
xstream					
Server-Side Request Forgery (SSRF)	16-Dec-20	5	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, a Server-Side Forgery Request vulnerability can be activated when unmarshalling. The vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist if running Java 15 or higher. No user is affected who followed the recommendation to setup XStream's Security Framework with a	https://github.com/x-stream/xstream/security/advisories/GHSA-4cch-wxpw-8p28	A-XST-XSTR-040121/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whilelist for the allowed types to avoid the vulnerability. Users of XStream 1.4.14 or below who still want to use XStream default blacklist can use a workaround described in more detailed in the referenced advisories. **CVE ID : CVE-2020-26258**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Dec-20	6.4	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, is vulnerable to an Arbitrary File Deletion on the local host when unmarshalling. The vulnerability may allow a remote attacker to delete arbitrary know files on the host as log as the executing process has sufficient rights only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist running Java 15 or higher. No user is affected, who followed the recommendation to setup XStream's Security	https://github.com/x-stream/xstream/security/advisories/GHSA-jfvx-7wrx-43fh	A-XST-XSTR-040121/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whilelist for the allowed types to avoid the vulnerability. Users of XStream 1.4.14 or below who still want to use XStream default blacklist can use a workaround described in more detailed in the referenced advisories. **CVE ID : CVE-2020-26259**		
xuxueli					
xxl-job					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Dec-20	4.3	XXL-JOB 2.2.0 allows Stored XSS (in Add User) to bypass the 20-character limit via xxl-job-admin/src/main/java/com/xxl/job/admin/controller/UserController.java. **CVE ID : CVE-2020-29204**	N/A	A-XUX-XXL--040121/436
yunyecms					
yunyecms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-20	7.5	SQL injection vulnerability in yunyecms V2.0.1 via the selcart parameter. **CVE ID : CVE-2020-21377**	N/A	A-YUN-YUNY-040121/437
Zammad					
Zammad					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	28-Dec-20	4	An issue was discovered in Zammad before 3.4.1. Admin Users without a ticket.* permission can access Tickets. **CVE ID : CVE-2020-26028**	N/A	A-ZAM-ZAMM-040121/438
Incorrect Authorization	28-Dec-20	4	An issue was discovered in Zammad before 3.4.1. There are wrong authorization checks for impersonation requests via X-On-Behalf-Of. The authorization checks are performed for the actual user and not the one given in the X-On-Behalf-Of header. **CVE ID : CVE-2020-26029**	N/A	A-ZAM-ZAMM-040121/439
Improper Authentication	28-Dec-20	7.5	An issue was discovered in Zammad before 3.4.1. There is an authentication bypass in the SSO endpoint via a crafted header, when SSO is not configured. An attacker can create a valid and authenticated session that can be used to perform any actions in the name of other users. **CVE ID : CVE-2020-26030**	N/A	A-ZAM-ZAMM-040121/440
Incorrect Default Permissions	28-Dec-20	4	An issue was discovered in Zammad before 3.4.1. The global-search feature leaks Knowledge Base drafts to Knowledge Base readers (who are authenticated but have insufficient permissions). **CVE ID : CVE-2020-26031**	N/A	A-ZAM-ZAMM-040121/441

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	28-Dec-20	5	An SSRF issue was discovered in Zammad before 3.4.1. The SMS configuration interface for Massenversand is implemented in a way that renders the result of a test request to the User. An attacker can use this to request any URL via a GET request from the network interface of the server. This may lead to disclosure of information from intranet systems. **CVE ID : CVE-2020-26032**	N/A	A-ZAM-ZAMM-040121/442
Cross-Site Request Forgery (CSRF)	28-Dec-20	5.8	An issue was discovered in Zammad before 3.4.1. The Tag and Link REST API endpoints (for add and delete) lack a CSRF token check. **CVE ID : CVE-2020-26033**	N/A	A-ZAM-ZAMM-040121/443
N/A	28-Dec-20	4	An account-enumeration issue was discovered in Zammad before 3.4.1. The Create User functionality is implemented in a way that would enable an anonymous user to guess valid user email addresses. The application responds differently depending on whether the input supplied was recognized as associated with a valid user. **CVE ID : CVE-2020-26034**	N/A	A-ZAM-ZAMM-040121/444
Improper	28-Dec-20	3.5	An issue was discovered in	N/A	A-ZAM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Zammad before 3.4.1. There is Stored XSS via a Tags element in a TIcket. **CVE ID : CVE-2020-26035**		ZAMM-040121/445
Incorrect Authorization	28-Dec-20	4	An issue was discovered in Zammad before 3.5.1. An Agent with Customer permissions in a Group can bypass intended access control on internal Articles via the Ticket detail view. **CVE ID : CVE-2020-29158**	N/A	A-ZAM-ZAMM-040121/446
N/A	28-Dec-20	4	An issue was discovered in Zammad before 3.5.1. The default signup Role (for newly created Users) can be a privileged Role, if configured by an admin. This behvaior was unintended. **CVE ID : CVE-2020-29159**	N/A	A-ZAM-ZAMM-040121/447
Incorrect Authorization	28-Dec-20	5	An issue was discovered in Zammad before 3.5.1. A REST API call allows an attacker to change Ticket Article data in a way that defeats auditing. **CVE ID : CVE-2020-29160**	N/A	A-ZAM-ZAMM-040121/448
Zimbra					
collaboration					
Improper Restriction of XML External Entity Reference ('XXE')	17-Dec-20	4	In Zimbra Collaboration Suite Network Edition versions < 9.0.0 P10 and 8.8.15 P17, there exists an XXE vulnerability in the saml consumer store	https://wiki.zimbra.com/wiki/Security_Center, https://wik	A-ZIM-COLL-040121/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			extension, which is vulnerable to XXE attacks. This has been fixed in Zimbra Collaboration Suite Network edition 9.0.0 Patch 10 and 8.8.15 Patch 17. **CVE ID : CVE-2020-35123**	i.zimbra.com/wiki/Zimbra_Releases/8.8.15/P17, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P10, https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories	
zzcms					
zzcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	3.5	There is a XSS in the user login page in zzcms 2019. Users can inject js code by the referer header via user/login.php **CVE ID : CVE-2020-20285**	N/A	A-ZZC-ZZCM-040121/450
zzzcms					
zzzphp					
N/A	18-Dec-20	7.5	Eval injection vulnerability in the parserCommom method in the ParserTemplate class in zzz_template.php in zzzphp 1.7.2 allows remote attackers to execute arbitrary commands. **CVE ID : CVE-2020-20298**	N/A	A-ZZZ-ZZZP-040121/451
Operating System					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Apple					
macos					
N/A	16-Dec-20	3.6	The installer of the macOS Sensor for VMware Carbon Black Cloud prior to 3.5.1 handles certain files in an insecure way. A malicious actor who has local access to the endpoint on which a macOS sensor is going to be installed, may overwrite a limited number of files with output from the sensor installation. **CVE ID : CVE-2020-4008**	N/A	O-APP-MACO-040121/452
mac_os_x					
NULL Pointer Dereference	21-Dec-20	2.1	VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition. **CVE ID : CVE-2020-3999**	N/A	O-APP-MAC_-040121/453
Canonical					
ubuntu_linux					
Loop with	26-Dec-20	4.3	GNOME gdk-pixbuf (aka	https://bug	O-CAN-UBUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unreachable Exit Condition ('Infinite Loop')			GdkPixbuf) before 2.42.2 allows a denial of service (infinite loop) in lzw.c in the function write_indexes. if c->self_code equals 10, self->code_table[10].extends will assign the value 11 to c. The next execution in the loop will assign self->code_table[11].extends to c, which will give the value of 10. This will make the loop run infinitely. This bug can, for example, be triggered by calling this function with a GIF image with LZW compression that is crafted in a special way. **CVE ID : CVE-2020-29385**	s.debian.org/cgi-bin/bugreport.cgi?bug=977166, https://gitlab.gnome.org/GNOME/gdk-pixbuf/-/issues/164, https://ubuntu.com/security/CVE-2020-29385	040121/454
Debian					
debian_linux					
Improper Encoding or Escaping of Output	18-Dec-20	5	In MediaWiki before 1.35.1, the messages userrights-expiry-current and userrights-expiry-none can contain raw HTML. XSS can happen when a user visits Special:UserRights but does not have rights to change all userrights, and the table on the left side has unchangeable groups in it. (The right column with the changeable groups is not affected and is escaped correctly.) **CVE ID : CVE-2020-35475**	N/A	O-DEB-DEBI-040121/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Dec-20	5	MediaWiki before 1.35.1 blocks legitimate attempts to hide log entries in some situations. If one sets MediaWiki:Mainpage to Special:MyLanguage/Main Page, visits a log entry on Special:Log, and toggles the "Change visibility of selected log entries" checkbox (or a tags checkbox) next to it, there is a redirection to the main page's action=historysubmit (instead of the desired behavior in which a revision-deletion form appears). **CVE ID : CVE-2020-35477**	N/A	O-DEB-DEBI-040121/456
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-20	4.3	MediaWiki before 1.35.1 allows XSS via BlockLogFormatter.php. Language::translateBlockExpiry itself does not escape in all code paths. For example, the return of Language::userTimeAndDate is is always unsafe for HTML in a month value. This affects MediaWiki 1.12.0 and later. **CVE ID : CVE-2020-35479**	N/A	O-DEB-DEBI-040121/457
Information Exposure	18-Dec-20	5	An issue was discovered in MediaWiki before 1.35.1. Missing users (accounts that don't exist) and hidden users (accounts that have been explicitly hidden due to being	N/A	O-DEB-DEBI-040121/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abusive, or similar) that the viewer cannot see are handled differently, exposing sensitive information about the hidden status to unprivileged viewers. This exists on various code paths. **CVE ID : CVE-2020-35480**		
Uncontrolled Resource Consumption	20-Dec-20	5	srs2.c in PostSRSd before 1.10 allows remote attackers to cause a denial of service (CPU consumption) via a long timestamp tag in an SRS address. **CVE ID : CVE-2020-35573**	N/A	O-DEB-DEBI-040121/459
Dell					
idrac9_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	Dell EMC iDRAC9 versions prior to 4.32.10.00 and 4.40.00.00 contain a reflected cross-site scripting vulnerability in the iDRAC9 web application. A remote attacker could potentially exploit this vulnerability to run malicious HTML or JavaScript in a victim's browser by tricking a victim in to following a specially crafted link. **CVE ID : CVE-2020-26198**	N/A	O-DEL-IDRA-040121/460
D-link					
dsl2888a_firmware					
Incorrect	22-Dec-20	3.3	An issue was discovered on	https://ww	O-D-L-DSL2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permission Assignment for Critical Resource			D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It has a misconfigured FTP service that allows a malicious network user to access system folders and download sensitive files (such as the password hash file). **CVE ID : CVE-2020-24578**	w.trustwave.com/en-us/resources/security-resources/security-advisories/	040121/461
Improper Authentication	22-Dec-20	5.8	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. An unauthenticated attacker could bypass authentication to access authenticated pages and functionality. **CVE ID : CVE-2020-24579**	https://www.trustwave.com/en-us/resources/security-resources/security-advisories/	O-D-L-DSL2-040121/462
Improper Authentication	22-Dec-20	5.4	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. Lack of authentication functionality allows an attacker to assign a static IP address that was once used by a valid user. **CVE ID : CVE-2020-24580**	https://www.trustwave.com/en-us/resources/security-resources/security-advisories/	O-D-L-DSL2-040121/463
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Dec-20	7.7	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It contains an execute_cmd.cgi feature (that is not reachable via the web user interface)	https://www.trustwave.com/en-us/resources/security-resources/security-	O-D-L-DSL2-040121/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that lets an authenticated user execute Operating System commands. **CVE ID : CVE-2020-24581**	advisories/	
Emerson					
x-stream_enhanced_xegp_firmware					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**	N/A	O-EME-X-ST-040121/465
x-stream_enhanced_xegk_firmware					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**	N/A	O-EME-X-ST-040121/466
x-stream_enhanced_xefd_firmware					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-	N/A	O-EME-X-ST-040121/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**		
x-stream_enhanced_xexf_firmware					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**	N/A	O-EME-X-ST-040121/468
Epson					
eps_tse_server_8_firmware					
Insufficiently Protected Credentials	16-Dec-20	7.5	Unrestricted access to the log downloader functionality in EPSON EPS TSE Server 8 (21.0.11) allows an unauthenticated attacker to remotely retrieve administrative hashed credentials via the maintenance/troubleshoot.	N/A	O-EPS-EPS_-040121/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			php?download=1 URI. **CVE ID : CVE-2020-28929**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	3.5	A Cross-Site Scripting (XSS) issue in the 'update user' and 'delete user' functionalities in settings/users.php in EPSON EPS TSE Server 8 (21.0.11) allows an authenticated attacker to inject a JavaScript payload in the user management page that is executed by an administrator. **CVE ID : CVE-2020-28930**	N/A	O-EPS-EPS_-040121/470
Cross-Site Request Forgery (CSRF)	16-Dec-20	6.8	Lack of an anti-CSRF token in the entire administrative interface in EPSON EPS TSE Server 8 (21.0.11) allows an unauthenticated attacker to force an administrator to execute external POST requests by visiting a malicious website. **CVE ID : CVE-2020-28931**	N/A	O-EPS-EPS_-040121/471
foscammall					
foscam_x1_firmware					
N/A	28-Dec-20	7.2	FOSCAM FHD X1 1.14.2.4 devices allow attackers (with physical UART access) to login via the ipc.fos~ password. **CVE ID : CVE-2020-28096**	N/A	O-FOS-FOSC-040121/472
Google					
android					
N/A	18-Dec-20	2.1	An issue was discovered in	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Finder on Samsung mobile devices with Q(10.0) software. A call to a non-existent provider allows attackers to cause a denial of service. The Samsung ID is SVE-2020-18629 (December 2020). **CVE ID : CVE-2020-35548**		040121/473
N/A	18-Dec-20	2.1	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Any application may establish itself as the default dialer, without user interaction. The Samsung ID is SVE-2020-19172 (December 2020). **CVE ID : CVE-2020-35549**	N/A	O-GOO-ANDR-040121/474
N/A	18-Dec-20	7.5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. Attackers can bypass Factory Reset Protection (FRP) via StatusBar. The Samsung ID is SVE-2020-17888 (December 2020). **CVE ID : CVE-2020-35550**	N/A	O-GOO-ANDR-040121/475
Authentication Bypass by Capture-replay	18-Dec-20	7.5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. They allow attackers to conduct RPMB state-change attacks because an unauthorized	N/A	O-GOO-ANDR-040121/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RPMB write operation can be replayed, a related issue to CVE-2020-13799. The Samsung ID is SVE-2020-18100 (December 2020). **CVE ID : CVE-2020-35551**		
N/A	18-Dec-20	5	An issue was discovered in the GPS daemon on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (non-Qualcomm chipsets) software. Attackers can obtain sensitive location information because the configuration file is incorrect. The Samsung ID is SVE-2020-18678 (December 2020). **CVE ID : CVE-2020-35552**	N/A	O-GOO-ANDR-040121/477
Improper Restriction of Power Consumption	18-Dec-20	7.8	An issue was discovered on Samsung mobile devices with Q(10.0) and R(11.0) (Qualcomm SM8250 chipsets) software. They allows attackers to cause a denial of service (unlock failure) by triggering a power-shortage incident that causes a false-positive attack detection. The Samsung ID is SVE-2020-19678 (December 2020). **CVE ID : CVE-2020-35553**	N/A	O-GOO-ANDR-040121/478
N/A	18-Dec-20	4.6	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10 software. There is a WebView SSL error-	N/A	O-GOO-ANDR-040121/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handler vulnerability. The LG ID is LVE-SMP-200026 (December 2020). **CVE ID : CVE-2020-35554**		
N/A	18-Dec-20	4.4	An issue was discovered on LG mobile devices with Android OS 10 software. When a dual-screen configuration is supported, the device does not lock upon disconnection of a call with the cover closed. The LG ID is LVE-SMP-200027 (December 2020). **CVE ID : CVE-2020-35555**	N/A	O-GOO-ANDR-040121/480
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged:	N/A	O-GOO-ANDR-040121/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
HP					
hp-ux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition 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: 186094. **CVE ID : CVE-2020-4657**	https://www.ibm.com/support/pages/node/6382414	O-HP-HP-U-040121/482
Improper Neutralization of Input During Web Page	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This	https://www.ibm.com/support/pages/node/	O-HP-HP-U-040121/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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: 186095. **CVE ID : CVE-2020-4658**	6382416	
storeever_msl2024_firmware					
Cross-Site Request Forgery (CSRF)	18-Dec-20	6.8	A potential security vulnerability has been identified in the HPE StoreEver MSL2024 Tape Library and HPE StoreEver 1/8 G2 Tape Autoloaders. The vulnerability could be remotely exploited to allow Cross-site Request Forgery (CSRF). **CVE ID : CVE-2020-7201**	N/A	O-HP-STOR-040121/484
storeever_1\/8_g2_tape_autoloader_firmware					
Cross-Site Request Forgery (CSRF)	18-Dec-20	6.8	A potential security vulnerability has been identified in the HPE StoreEver MSL2024 Tape Library and HPE StoreEver 1/8 G2 Tape Autoloaders. The vulnerability could be remotely exploited to allow Cross-site Request Forgery (CSRF). **CVE ID : CVE-2020-7201**	N/A	O-HP-STOR-040121/485
Huawei					
honor_20_pro_firmware					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some	https://www.huawei.c	O-HUA-HONO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Huawei smartphones. Due to the improper processing of received abnormal messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	om/en/psirt/security-advisories/huawei-sa-20201216-03-smartphone-en	040121/486
cloudengine_6800_firmware					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	O-HUA-CLOU-040121/487
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-cloudengine-en	O-HUA-CLOU-040121/488
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine	N/A	O-HUA-CLOU-040121/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**		
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	O-HUA-CLOU-040121/490
mate_30_pro_firmware					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion.	N/A	O-HUA-MATE-040121/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9119		
cloudengine_5800_firmware					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	O-HUA-CLOU-040121/492
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-cloudengine-en	O-HUA-CLOU-040121/493
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the	N/A	O-HUA-CLOU-040121/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**		
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	O-HUA-CLOU-040121/495
cloudengine_7800_firmware					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	O-HUA-CLOU-040121/496
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-	O-HUA-CLOU-040121/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	cloudengine-en	
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**	N/A	O-HUA-CLOU-040121/498
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	O-HUA-CLOU-040121/499
jackman-al00d_firmware					
Uncontrolled	29-Dec-20	2.1	There is a resource	https://ww	O-HUA-JACK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			management error vulnerability in Jackman-AL00D versions 8.2.0.185(C00R2P1). Local attackers construct malicious application files, causing system applications to run abnormally. **CVE ID : CVE-2020-1848**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-02-smartphone-en	040121/500
yale-l21a_firmware					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-03-smartphone-en	O-HUA-YALE-040121/501
yale-l61a_firmware					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-03-smartphone-en	O-HUA-YALE-040121/502
p40_firmware					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart	N/A	O-HUA-P40_-040121/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**		
p40_pro_firmware					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**	N/A	O-HUA-P40_-040121/504
princeton-al10d_firmware					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-03-smartphone-en	O-HUA-PRIN-040121/505
cloudengine_12800_firmware					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei	https://www.huawei.com/en/psir	O-HUA-CLOU-040121/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	t/security-advisories/huawei-sa-20201216-01-obr-en	
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-cloudengine-en	O-HUA-CLOU-040121/507
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**	N/A	O-HUA-CLOU-040121/508
Improper	29-Dec-20	6.8	There is an improper	https://ww	O-HUA-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	040121/509
nip6800_firmware					
Out-of-bounds Read	24-Dec-20	3.3	There is an out-of-bounds read vulnerability in some versions of NIP6800, Secospace USG6600 and USG9500. The software reads data past the end of the intended buffer when parsing DHCP messages including crafted parameter. Successful exploit could cause certain service abnormal. **CVE ID : CVE-2020-9201**	N/A	O-HUA-NIP6-040121/510
secospace_usg6600_firmware					
Out-of-bounds Read	24-Dec-20	3.3	There is an out-of-bounds read vulnerability in some versions of NIP6800, Secospace USG6600 and USG9500. The software reads data past the end of the intended buffer when parsing DHCP messages including crafted parameter. Successful	N/A	O-HUA-SECO-040121/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could cause certain service abnormal. **CVE ID : CVE-2020-9201**		
taurus-al00a_firmware					
Use After Free	29-Dec-20	4.3	There is a use after free vulnerability in Taurus-AL00A versions 10.0.0.1(C00E1R1P1). A module does not deal with specific message properly, which makes a function refer to memory after it has been freed. Attackers can exploit this vulnerability by running a crafted application with common privilege. This would compromise normal service. **CVE ID : CVE-2020-9093**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-smartphone-en	O-HUA-TAUR-040121/512
mate_10_firmware					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**	N/A	O-HUA-MATE-040121/513
mate_30_firmware					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design	N/A	O-HUA-MATE-040121/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**		
Out-of-bounds Read	29-Dec-20	4.6	There is an out-of-bound read vulnerability in huawei smartphone Mate 30 versions earlier than 10.1.0.156 (C00E155R7P2). An attacker with specific permission can exploit this vulnerability by sending crafted packet with specific parameter to the target device. Due to insufficient validation of the parameter, successful exploit can cause the device to behave abnormally. **CVE ID : CVE-2020-9125**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-taurus-en	O-HUA-MATE-040121/515
usg9500_firmware					
Out-of-bounds Read	24-Dec-20	3.3	There is an out-of-bounds read vulnerability in some versions of NIP6800, Secospace USG6600 and USG9500. The software reads data past the end of the intended buffer when parsing DHCP messages including crafted parameter. Successful exploit could cause certain service abnormal.	N/A	O-HUA-USG9-040121/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9201		
IBM					
AIX					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition 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: 186094. **CVE ID : CVE-2020-4657**	https://www.ibm.com/support/pages/node/6382414	O-IBM-AIX-040121/517
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186095. **CVE ID : CVE-2020-4658**	https://www.ibm.com/support/pages/node/6382416	O-IBM-AIX-040121/518
Improper Neutralization of Input During Web Page Generation ('Cross-site	21-Dec-20	3.5	IBM FileNet Content Manager and IBM Content Navigator 3.0.CD is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary	https://www.ibm.com/support/pages/node/6388806	O-IBM-AIX-040121/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 188600. **CVE ID : CVE-2020-4757**		
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	O-IBM-AIX-040121/520
i					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition 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: 186094. **CVE ID : CVE-2020-4657**	https://www.ibm.com/support/pages/node/6382414	O-IBM-I-040121/521
Improper Neutralization of Input During Web Page Generation	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users	https://www.ibm.com/support/pages/node/6382416	O-IBM-I-040121/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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: 186095. **CVE ID : CVE-2020-4658**		
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	O-IBM-I-040121/523
linux_on_zseries					
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	O-IBM-LINU-040121/524
kyland					
kps2204_6_port_managed_din-rail_programmable_serial_device_firmware					
Unrestricted Upload of File with Dangerous Type	17-Dec-20	7.5	An arbitrary code execution vulnerability in Kyland KPS2204 6 Port Managed Din-Rail Programmable Serial Device Servers Software Version:R0002.P05 allows	N/A	O-KYL-KPS2-040121/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to upload a malicious script file by constructing a POST type request and writing a payload in the request parameters as an instruction to write a file. **CVE ID : CVE-2020-25010**		
Insufficiently Protected Credentials	17-Dec-20	5	A sensitive information disclosure vulnerability in Kyland KPS2204 6 Port Managed Din-Rail Programmable Serial Device Servers Software Version:R0002.P05 allows remote attackers to get username and password by request /cgi-bin/webadminget.cgi script via the browser. **CVE ID : CVE-2020-25011**	N/A	O-KYL-KPS2-040121/526
Lantronix					
xport_edge_firmware					
Improper Authentication	18-Dec-20	4	An authentication bypass vulnerability exists in the Web Manager functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause increased privileges. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-13527**	N/A	O-LAN-XPOR-040121/527
Cleartext Transmission	18-Dec-20	4.3	An information disclosure vulnerability exists in the	N/A	O-LAN-XPOR-040121/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Information			Web Manager and telnet CLI functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause information disclosure. An attacker can sniff the network to trigger this vulnerability. **CVE ID : CVE-2020-13528**		
sgx_firmware					
Improper Authentication	18-Dec-20	4	An authentication bypass vulnerability exists in the Web Manager functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause increased privileges. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-13527**	N/A	O-LAN-SGX_-040121/529
Linksys					
re6500_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-20	10	Belkin LINKSYS RE6500 devices before 1.0.012.001 allow remote attackers to execute arbitrary commands or set a new password via shell metacharacters to the goform/setSysAdm page. **CVE ID : CVE-2020-35713**	N/A	O-LIN-RE65-040121/530
Improper	26-Dec-20	6.5	Belkin LINKSYS RE6500	N/A	O-LIN-RE65-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			devices before 1.0.11.001 allow remote authenticated users to execute arbitrary commands via goform/systemCommand?command= in conjunction with the goform/pingstart program. **CVE ID : CVE-2020-35714**		040121/531
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-20	9	Belkin LINKSYS RE6500 devices before 1.0.012.001 allow remote authenticated users to execute arbitrary commands via shell metacharacters in a filename to the upload_settings.cgi page. **CVE ID : CVE-2020-35715**	N/A	O-LIN-RE65-040121/532
N/A	26-Dec-20	7.8	Belkin LINKSYS RE6500 devices before 1.0.012.001 allow remote attackers to cause a persistent denial of service (segmentation fault) via a long /goform/langSwitch langSelectionOnly parameter. **CVE ID : CVE-2020-35716**	N/A	O-LIN-RE65-040121/533
Linux					
linux_kernel					
Server-Side Request Forgery (SSRF)	26-Dec-20	9.3	Esri ArcGIS Server before 10.8 is vulnerable to SSRF in some configurations. **CVE ID : CVE-2020-35712**	N/A	O-LIN-LINU-040121/534
N/A	23-Dec-20	2.1	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5	https://www.ibm.com/support/pages/node/	O-LIN-LINU-040121/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow local attacker to cause a denial of service inside the "DB2 Management Service". **CVE ID : CVE-2020-4642**	6391652	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition 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: 186094. **CVE ID : CVE-2020-4657**	https://www.ibm.com/support/pages/node/6382414	O-LIN-LINU-040121/536
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186095. **CVE ID : CVE-2020-4658**	https://www.ibm.com/support/pages/node/6382416	O-LIN-LINU-040121/537
Improper Neutralization of Input During Web Page Generation	21-Dec-20	3.5	IBM FileNet Content Manager and IBM Content Navigator 3.0.CD is vulnerable to stored cross-site scripting. This	https://www.ibm.com/support/pages/node/6388806	O-LIN-LINU-040121/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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: 188600. **CVE ID : CVE-2020-4757**		
Cross-Site Request Forgery (CSRF)	18-Dec-20	4.3	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 188898. **CVE ID : CVE-2020-4764**	https://www.ibm.com/support/pages/node/6386492	O-LIN-LINU-040121/539
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	O-LIN-LINU-040121/540
mersive					
solstice_pod_firmware					
N/A	23-Dec-20	4.3	In Solstice Pod before 3.0.3, the web services allow users to connect to them over unencrypted channels via the Browser Look-in feature. An attacker suitably positioned to view	N/A	O-MER-SOLS-040121/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a legitimate user's network traffic could record and monitor their interactions with the web services and obtain any information the user supplies, including Administrator passwords and screen keys. **CVE ID : CVE-2020-35584**		
Improper Restriction of Excessive Authentication Attempts	23-Dec-20	5	In Solstice Pod before 3.3.0 (or Open4.3), the screen key can be enumerated using brute-force attacks via the /lookin/info Solstice Open Control API because there are only 1.7 million possibilities. **CVE ID : CVE-2020-35585**	N/A	O-MER-SOLS-040121/542
Improper Restriction of Excessive Authentication Attempts	23-Dec-20	5	In Solstice Pod before 3.3.0 (or Open4.3), the Administrator password can be enumerated using brute-force attacks via the /Config/service/initModel?password= Solstice Open Control API because there is no complexity requirement (e.g., it might be all digits or all lowercase letters). **CVE ID : CVE-2020-35586**	N/A	O-MER-SOLS-040121/543
solstice_firmware					
N/A	23-Dec-20	5	** DISPUTED ** In Solstice Pod before 3.0.3, the firmware can easily be decompiled/disassembled. The decompiled/disassembled files contain non-	N/A	O-MER-SOLS-040121/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obfuscated code. NOTE: it is unclear whether lack of obfuscation is directly associated with a negative impact, or instead only facilitates an attack technique. **CVE ID : CVE-2020-35587**		
Microsoft					
windows					
Incorrect Permission Assignment for Critical Resource	24-Dec-20	6.9	The td-agent-builder plugin before 2020-12-18 for Fluentd allows attackers to gain privileges because the bin directory is writable by a user account, but a file in bin is executed as NT AUTHORITY\SYSTEM. **CVE ID : CVE-2020-28169**	https://github.com/fluent/fluentd/issues/3201, https://github.com/fluent-plugins-nursery/td-agent-builder/pull/247/commits/6f9cb6393392d62caa99907c0ebbcbab6b94a3f1, https://github.com/kenhys/td-agent-builder/commit/eec6e2dedf12f2e0c01c2bbe7b8c15b639b3b938	O-MIC-WIND-040121/545
N/A	24-Dec-20	4.4	With MariaDB running on	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows, when local clients connect to the server over named pipes, it's possible for an unprivileged user with an ability to run code on the server machine to intercept the named pipe connection and act as a man-in-the-middle, gaining access to all the data passed between the client and the server, and getting the ability to run SQL commands on behalf of the connected user. This occurs because of an incorrect security descriptor. This affects MariaDB Server before 10.1.48, 10.2.x before 10.2.35, 10.3.x before 10.3.26, 10.4.x before 10.4.16, and 10.5.x before 10.5.7. NOTE: this issue exists because certain details of the MariaDB CVE-2019-2503 fix did not comprehensively address attack variants against MariaDB. This situation is specific to MariaDB, and thus CVE-2020-28912 does NOT apply to other vendors that were originally affected by CVE-2019-2503. **CVE ID : CVE-2020-28912**		040121/546
Server-Side Request	26-Dec-20	9.3	Esri ArcGIS Server before 10.8 is vulnerable to SSRF	N/A	O-MIC-WIND-040121/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			in some configurations. **CVE ID : CVE-2020-35712**		
N/A	29-Dec-20	7.5	miniserv.pl in Webmin 1.962 on Windows mishandles special characters in query arguments to the CGI program. **CVE ID : CVE-2020-35769**	N/A	O-MIC-WIND-040121/548
N/A	23-Dec-20	2.1	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow local attacker to cause a denial of service inside the "DB2 Management Service". **CVE ID : CVE-2020-4642**	https://www.ibm.com/support/pages/node/6391652	O-MIC-WIND-040121/549
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition 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: 186094. **CVE ID : CVE-2020-4657**	https://www.ibm.com/support/pages/node/6382414	O-MIC-WIND-040121/550
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	https://www.ibm.com/support/pages/node/6382416	O-MIC-WIND-040121/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186095. **CVE ID : CVE-2020-4658**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-20	3.5	IBM FileNet Content Manager and IBM Content Navigator 3.0.CD is vulnerable to stored 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: 188600. **CVE ID : CVE-2020-4757**	https://www.ibm.com/support/pages/node/6388806	O-MIC-WIND-040121/552
Cross-Site Request Forgery (CSRF)	18-Dec-20	4.3	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 188898. **CVE ID : CVE-2020-4764**	https://www.ibm.com/support/pages/node/6386492	O-MIC-WIND-040121/553
URL Redirection to Untrusted Site ('Open Redirect')	21-Dec-20	5.8	IBM Security Secret Server 10.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit	https://www.ibm.com/support/pages/node/6336251	O-MIC-WIND-040121/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 190044. **CVE ID : CVE-2020-4840**		
Information Exposure	21-Dec-20	4.3	IBM Security Secret Server 10.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 190045. **CVE ID : CVE-2020-4841**	https://www.ibm.com/support/pages/node/6336251	O-MIC-WIND-040121/555
Information Exposure Through an Error Message	21-Dec-20	4	IBM Security Secret Server 10.6 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 190046. **CVE ID : CVE-2020-4842**	https://www.ibm.com/support/pages/node/6336251	O-MIC-WIND-040121/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	21-Dec-20	4	IBM Security Secret Server 10.6 stores potentially sensitive information in config files that could be read by an authenticated user. IBM X-Force ID: 190048. **CVE ID : CVE-2020-4843**	https://www.ibm.com/support/pages/node/6250375	O-MIC-WIND-040121/557
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	O-MIC-WIND-040121/558
Improper Input Validation	18-Dec-20	6.8	A arbitrary code execution vulnerability exists in the way that the Stove client improperly validates input value. An attacker could execute arbitrary code when the user access to crafted web page. This issue affects: Smilegate STOVE Client 0.0.4.72. **CVE ID : CVE-2020-7838**	N/A	O-MIC-WIND-040121/559
Mitel					
6873i_sip_firmware					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth	N/A	O-MIT-6873-040121/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27639**		
6930_sip_firmware					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27639**	N/A	O-MIT-6930-040121/561
6940_sip_firmware					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an	N/A	O-MIT-6940-040121/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27639**		
mivoice_6940_firmware					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6940 and 6930 MiNet phones with firmware before 1.5.3 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27640**	N/A	O-MIT-MIVO-040121/563
mivoice_6930_firmware					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6940 and 6930 MiNet phones with firmware before 1.5.3 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27640**	N/A	O-MIT-MIVO-040121/564
Moxa					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nport_iaw5000a-i\/o_firmware					
Weak Password Requirements	23-Dec-20	5	The built-in web service for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower does not require users to have strong passwords. **CVE ID : CVE-2020-25153**	N/A	O-MOX-NPOR-040121/565
Cleartext Transmission of Sensitive Information	23-Dec-20	5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower stores and transmits the credentials of third-party services in cleartext. **CVE ID : CVE-2020-25190**	N/A	O-MOX-NPOR-040121/566
Information Exposure	23-Dec-20	5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower allows sensitive information to be displayed without proper authorization. **CVE ID : CVE-2020-25192**	N/A	O-MOX-NPOR-040121/567
Improper Privilege Management	23-Dec-20	6.5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower has improper privilege management, which may allow an attacker with user privileges to perform requests with administrative privileges. **CVE ID : CVE-2020-25194**	N/A	O-MOX-NPOR-040121/568
Improper Restriction of Excessive	23-Dec-20	5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1	N/A	O-MOX-NPOR-040121/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			or lower allows SSH/Telnet sessions, which may be vulnerable to brute force attacks to bypass authentication. **CVE ID : CVE-2020-25196**		
Session Fixation	23-Dec-20	6.8	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower has incorrectly implemented protections from session fixation, which may allow an attacker to gain access to a session and hijack it by stealing the user's cookies. **CVE ID : CVE-2020-25198**	N/A	O-MOX-NPOR-040121/570
Netgear					
rbk40_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-RBK4-040121/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35815		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RBK4-040121/572
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10.	N/A	O-NET-RBK4-040121/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35821		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-RBK4-040121/574
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	O-NET-RBK4-040121/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-RBK4-040121/576
rbr50_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before	N/A	O-NET-RBR5-040121/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RBR5-040121/578
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	O-NET-RBR5-040121/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-RBR5-040121/580
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	O-NET-RBR5-040121/581
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	O-NET-RBR5-040121/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-RBR5-040121/583
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-RBR5-040121/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-RBR5-040121/585
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before	N/A	O-NET-RBR5-040121/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-RBR5-040121/587
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	O-NET-RBR5-040121/588
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before	N/A	O-NET-RBR5-040121/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-RBR5-040121/590
rbs50_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	O-NET-RBS5-040121/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RBS5-040121/592
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	O-NET-RBS5-040121/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-RBS5-040121/594
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-RBS5-040121/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35820		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-RBS5-040121/596
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-RBS5-040121/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35805		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-RBS5-040121/598
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-RBS5-040121/599
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	O-NET-RBS5-040121/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-RBS5-040121/601
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	O-NET-RBS5-040121/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	O-NET-RBS5-040121/603
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-RBS5-040121/604
rbk50_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	O-NET-RBK5-040121/605
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	O-NET-RBK5-040121/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**	N/A	O-NET-RBK5-040121/607
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-RBK5-040121/608
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	O-NET-RBK5-040121/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-RBK5-040121/610
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before	N/A	O-NET-RBK5-040121/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-RBK5-040121/612
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-RBK5-040121/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-RBK5-040121/614
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-RBK5-040121/615
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	O-NET-RBK5-040121/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	O-NET-RBK5-040121/617
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before	N/A	O-NET-RBK5-040121/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
r6220_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R622-040121/619

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-R622-040121/620
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-R622-040121/621
r6260_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R626-040121/622
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before	N/A	O-NET-R626-040121/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-R626-040121/624
r6800_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before	N/A	O-NET-R680-040121/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
d7000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before	N/A	O-NET-D700-040121/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050	N/A	O-NET-D700-040121/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-D700-040121/628
d6200_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before	N/A	O-NET-D620-040121/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-D620-040121/630
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before	N/A	O-NET-D620-040121/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
pr2000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before	N/A	O-NET-PR20-040121/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r6050_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before	N/A	O-NET-R605-040121/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-R605-040121/634
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before	N/A	O-NET-R605-040121/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
jr6150_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-JR61-040121/636
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-JR61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		040121/637
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-JR61-040121/638
r6120_firmware					
Buffer Copy	30-Dec-20	5.2	Certain NETGEAR devices	N/A	O-NET-R612-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		040121/639
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5	N/A	O-NET-R612-040121/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-R612-040121/641
jgs516pe_firmware					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48,	N/A	O-NET-JGS5-040121/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**		
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**	N/A	O-NET-JGS5-040121/643
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	O-NET-JGS5-040121/644
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**	N/A	O-NET-JGS5-040121/645
rbk752_firmware					
Improper Neutralization of Special Elements used	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This	N/A	O-NET-RBK7-040121/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in a Command ('Command Injection')			affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**		
rbr750_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	O-NET-RBR7-040121/647
rbs750_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	O-NET-RBS7-040121/648
rbk852_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	O-NET-RBK8-040121/649
rbr850_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	O-NET-RBR8-040121/650
rbs850_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	N/A	O-NET-RBS8-040121/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-35794**		
r6020_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R602-040121/652
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	O-NET-R602-040121/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-R602-040121/654
r6080_firmware					
Buffer Copy without	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer	N/A	O-NET-R608-040121/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	O-NET-R608-040121/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-R608-040121/657
wnr2020_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	O-NET-WNR2-040121/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	O-NET-WNR2-040121/659
r7500v2_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-R750-040121/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-R750-040121/661
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-R750-040121/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-R750-040121/663
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	O-NET-R750-040121/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-R750-040121/665
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-R750-040121/666
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before	N/A	O-NET-R750-040121/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-R750-040121/668
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-R750-040121/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	O-NET-R750-040121/670
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	O-NET-R750-040121/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	O-NET-R750-040121/672
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	O-NET-R750-040121/673
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	O-NET-R750-040121/674

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ex7000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-EX70-040121/675
dgn2200_firmware					
Improper Authentication	30-Dec-20	5.8	NETGEAR DGN2200v1 devices before v1.0.0.60 mishandle HTTPd authentication (aka PSV-	N/A	O-NET-DGN2-040121/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0363, PSV-2020-0364, and PSV-2020-0365). **CVE ID : CVE-2020-35785**		
r6300_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R630-040121/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
r6700_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R670-040121/678
r6900p_firmware					
Buffer Copy without Checking Size of Input	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This	N/A	O-NET-R690-040121/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r6900_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before	N/A	O-NET-R690-040121/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r7000p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before	N/A	O-NET-R700-040121/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r7000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before	N/A	O-NET-R700-040121/682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
dgn2200v1_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	7.7	NETGEAR DGN2200v1 devices before v1.0.0.58 are affected by command injection. **CVE ID : CVE-2020-35777**	N/A	O-NET-DGN2-040121/683
gs716t_firmware					
Cross-Site Request Forgery (CSRF)	30-Dec-20	6.8	Certain NETGEAR devices are affected by CSRF. This affects GS716Tv3 before 6.3.1.36 and GS724Tv4 before 6.3.1.36. **CVE ID : CVE-2020-35778**	N/A	O-NET-GS71-040121/684
gs724t_firmware					
Cross-Site Request Forgery (CSRF)	30-Dec-20	6.8	Certain NETGEAR devices are affected by CSRF. This affects GS716Tv3 before 6.3.1.36 and GS724Tv4 before 6.3.1.36. **CVE ID : CVE-2020-35778**	N/A	O-NET-GS72-040121/685
nms300_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Dec-20	7.8	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service. **CVE ID : CVE-2020-35779**	N/A	O-NET-NMS3-040121/686
N/A	30-Dec-20	4	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service. **CVE ID : CVE-2020-35780**	N/A	O-NET-NMS3-040121/687
N/A	30-Dec-20	4	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service. **CVE ID : CVE-2020-35781**	N/A	O-NET-NMS3-040121/688
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	6.5	NETGEAR NMS300 devices before 1.6.0.27 are affected by command injection by an authenticated user. **CVE ID : CVE-2020-35789**	N/A	O-NET-NMS3-040121/689
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	7.5	NETGEAR NMS300 devices before 1.6.0.27 are affected by command injection by an unauthenticated attacker. **CVE ID : CVE-2020-35797**	N/A	O-NET-NMS3-040121/690
jgs524e_firmware					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**	N/A	O-NET-JGS5-040121/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**	N/A	O-NET-JGS5-040121/692
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	O-NET-JGS5-040121/693
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**	N/A	O-NET-JGS5-040121/694
d7800_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-D780-040121/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-D780-040121/696
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-D780-040121/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-D780-040121/698
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	O-NET-D780-040121/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-D780-040121/700
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-D780-040121/701
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26.	N/A	O-NET-D780-040121/702

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35790		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	O-NET-D780-040121/703
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**	N/A	O-NET-D780-040121/704
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-D780-040121/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-D780-040121/706
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-D780-040121/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35823		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-D780-040121/708
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-D780-040121/709
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-D780-040121/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	O-NET-D780-040121/711
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	O-NET-D780-040121/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	O-NET-D780-040121/713
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	O-NET-D780-040121/714
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	O-NET-D780-040121/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
r7500_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-R750-040121/716
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**	N/A	O-NET-R750-040121/717
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	O-NET-R750-040121/718
r7800_firmware					
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	O-NET-R780-040121/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-R780-040121/720
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-R780-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		040121/721
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-R780-040121/722
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-R780-040121/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-R780-040121/724
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-R780-040121/725
Buffer Copy without Checking Size of Input	30-Dec-20	2.7	NETGEAR R7800 devices before 1.0.2.74 are affected by a buffer overflow by an authenticated user.	N/A	O-NET-R780-040121/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2020-35786**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R780-040121/727
Improper Neutralization of Special Elements used	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This	N/A	O-NET-R780-040121/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in a Command ('Command Injection')			affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26. **CVE ID : CVE-2020-35790**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35791**	N/A	O-NET-R780-040121/729
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**	N/A	O-NET-R780-040121/730
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	O-NET-R780-040121/731
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information.	N/A	O-NET-R780-040121/732

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-R780-040121/733
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	O-NET-R780-040121/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-R780-040121/735
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-R780-040121/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-R780-040121/737
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	O-NET-R780-040121/738
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before	N/A	O-NET-R780-040121/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-R780-040121/740
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	O-NET-R780-040121/741
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	O-NET-R780-040121/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	O-NET-R780-040121/743
r8900_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before	N/A	O-NET-R890-040121/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-R890-040121/745
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-R890-040121/746

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35817		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-R890-040121/747
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	O-NET-R890-040121/748
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before	N/A	O-NET-R890-040121/749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-R890-040121/750
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before	N/A	O-NET-R890-040121/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26. **CVE ID : CVE-2020-35790**	N/A	O-NET-R890-040121/752
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35791**	N/A	O-NET-R890-040121/753
Improper Neutralization of Special	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an	N/A	O-NET-R890-040121/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	O-NET-R890-040121/755
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**	N/A	O-NET-R890-040121/756
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before	N/A	O-NET-R890-040121/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-R890-040121/758
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before	N/A	O-NET-R890-040121/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-R890-040121/760
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-R890-040121/761
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	O-NET-R890-040121/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	O-NET-R890-040121/763
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before	N/A	O-NET-R890-040121/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	O-NET-R890-040121/765
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	O-NET-R890-040121/766
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-R890-040121/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**		
r9000_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	O-NET-R900-040121/768
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before	N/A	O-NET-R900-040121/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**	N/A	O-NET-R900-040121/770
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-R900-040121/771
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-R900-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**		040121/772
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-R900-040121/773
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	O-NET-R900-040121/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-R900-040121/775
Improper	30-Dec-20	5.2	Certain NETGEAR devices	N/A	O-NET-R900-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26. **CVE ID : CVE-2020-35790**		040121/776
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35791**	N/A	O-NET-R900-040121/777
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**	N/A	O-NET-R900-040121/778
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	O-NET-R900-040121/779

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**	N/A	O-NET-R900-040121/780
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-R900-040121/781
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before	N/A	O-NET-R900-040121/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-R900-040121/783
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	O-NET-R900-040121/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-R900-040121/785
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	O-NET-R900-040121/786
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before	N/A	O-NET-R900-040121/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-R900-040121/788
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-R900-040121/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35835		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	O-NET-R900-040121/790
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	O-NET-R900-040121/791
rax120_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before	N/A	O-NET-RAX1-040121/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RAX1-040121/793
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-RAX1-040121/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-RAX1-040121/795
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	O-NET-RAX1-040121/796
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-RAX1-040121/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-RAX1-040121/798
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before	N/A	O-NET-RAX1-040121/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-RAX1-040121/800
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	O-NET-RAX1-040121/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-RAX1-040121/802
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-RAX1-040121/803
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-RAX1-040121/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	O-NET-RAX1-040121/805
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-RAX1-040121/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	O-NET-RAX1-040121/807
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	O-NET-RAX1-040121/808
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-RAX1-040121/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35838		
xr500_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	O-NET-XR50-040121/810
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-XR50-040121/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**	N/A	O-NET-XR50-040121/812
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-XR50-040121/813
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	O-NET-XR50-040121/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-XR50-040121/815
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before	N/A	O-NET-XR50-040121/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-XR50-040121/817
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	O-NET-XR50-040121/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-XR50-040121/819
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	O-NET-XR50-040121/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	O-NET-XR50-040121/821
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	O-NET-XR50-040121/822
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-XR50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		040121/823
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-XR50-040121/824
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-XR50-040121/825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	O-NET-XR50-040121/826
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	O-NET-XR50-040121/827
xr700_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-XR70-040121/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-XR70-040121/829
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-XR70-040121/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	O-NET-XR70-040121/831
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	O-NET-XR70-040121/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-XR70-040121/833
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	O-NET-XR70-040121/834
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34.	N/A	O-NET-XR70-040121/835

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35804		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-XR70-040121/836
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	O-NET-XR70-040121/837
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	O-NET-XR70-040121/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	O-NET-XR70-040121/839
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	O-NET-XR70-040121/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	O-NET-XR70-040121/841
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	O-NET-XR70-040121/842
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-XR70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		040121/843
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	O-NET-XR70-040121/844
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	O-NET-XR70-040121/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	O-NET-XR70-040121/846
rbr20_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	O-NET-RBR2-040121/847
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-RBR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		040121/848
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-RBR2-040121/849
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	O-NET-RBR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		040121/850
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	O-NET-RBR2-040121/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35823		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-RBR2-040121/852
rbs20_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	O-NET-RBS2-040121/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RBS2-040121/854
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before	N/A	O-NET-RBS2-040121/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-RBS2-040121/856
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before	N/A	O-NET-RBS2-040121/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-RBS2-040121/858
rbk20_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before	N/A	O-NET-RBK2-040121/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RBK2-040121/860
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before	N/A	O-NET-RBK2-040121/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-RBK2-040121/862
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before	N/A	O-NET-RBK2-040121/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	O-NET-RBK2-040121/864
rbr40_firmware					
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	O-NET-RBR4-040121/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-RBR4-040121/866
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	O-NET-RBR4-040121/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-RBR4-040121/868
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	O-NET-RBR4-040121/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
rbs40_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	O-NET-RBS4-040121/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	O-NET-RBS4-040121/871
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	O-NET-RBS4-040121/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	O-NET-RBS4-040121/873
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	O-NET-RBS4-040121/874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35830**		
jgs524pe_firmware					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**	N/A	O-NET-JGS5-040121/875
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**	N/A	O-NET-JGS5-040121/876
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	O-NET-JGS5-040121/877
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48,	N/A	O-NET-JGS5-040121/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**		
gs116e_firmware					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**	N/A	O-NET-GS11-040121/879
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**	N/A	O-NET-GS11-040121/880
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	O-NET-GS11-040121/881
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect	N/A	O-NET-GS11-040121/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**		
d3600_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before	N/A	O-NET-D360-040121/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
d6000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-D600-040121/884
ex6200_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	O-NET-EX62-040121/885
ex8000_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before	N/A	O-NET-EX80-040121/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
wac104_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	NETGEAR WAC104 devices before 1.0.4.13 are affected by a buffer overflow by an authenticated user. **CVE ID : CVE-2020-35788**	N/A	O-NET-WAC1-040121/887
rbs40v_firmware					
Improper Neutralization	30-Dec-20	5.2	Certain NETGEAR devices are affected by command	N/A	O-NET-RBS4-040121/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Special Elements used in a Command ('Command Injection')			injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**		
jnr1010v2_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-JNR1-040121/889
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	O-NET-JNR1-040121/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
jwnr2010v5_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-JWNR-040121/891
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	O-NET-JWNR-040121/892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
wnr1000v4_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-WNR1-040121/893
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	O-NET-WNR1-040121/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
wnr2050_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	O-NET-WNR2-040121/895
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	O-NET-WNR2-040121/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
Oracle					
solaris					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling B2B Integrator 5.2.0.0 through 6.0.3.2 Standard Edition 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: 186094. **CVE ID : CVE-2020-4657**	https://www.ibm.com/support/pages/node/6382414	O-ORA-SOLA-040121/897
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure	https://www.ibm.com/support/pages/node/6382416	O-ORA-SOLA-040121/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			within a trusted session. IBM X-Force ID: 186095. **CVE ID : CVE-2020-4658**		
N/A	21-Dec-20	5	IBM MQ 9.2 CD and LTS are vulnerable to a denial of service attack caused by an error processing connecting applications. IBM X-Force ID: 190833. **CVE ID : CVE-2020-4870**	https://www.ibm.com/support/pages/node/6380742, https://www.ibm.com/support/pages/node/6386466	O-ORA-SOLA-040121/899
Panasonic					
wv-s2231l_firmware					
Use of Hard-coded Credentials	28-Dec-20	2.1	Panasonic Security System WV-S2231L 4.25 has an insecure hard-coded password of lkjhgfdsa (which is just the asdf keyboard row in reverse order). **CVE ID : CVE-2020-29193**	N/A	O-PAN-WV-S-040121/900
N/A	28-Dec-20	5	Panasonic Security System WV-S2231L 4.25 allows a denial of service of the admin control panel (which will require a physical reset to restore administrative control) via Randomnum=99AC8CEC6E845B28&mode=1 in a POST request to the cgi-bin/set_factory URI. **CVE ID : CVE-2020-29194**	N/A	O-PAN-WV-S-040121/901
Phoenixcontact					
tc_mguard_rs4000_4g_vpn_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-TC_M-040121/902
innominate_mguard_rs4000_4tx\/tx_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-INNO-040121/903
innominate_mguard_rs4000_4tx\/tx_vpn_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get	https://cert.vde.com/en-	O-PHO-INNO-040121/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	us/advisories/vde-2020-046	
innominate_mguard_rs4000_4tx\/3g\/tx_vpn_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-INNO-040121/905
plcnext_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript	https://cert.vde.com/en-us/advisories/vde-2020-049	O-PHO-PLCN-040121/906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**		
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks. **CVE ID : CVE-2020-12518**	https://cert.vde.com/en-us/advisories/vde-2020-049	O-PHO-PLCN-040121/907
Improper Privilege Management	17-Dec-20	10	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges. **CVE ID : CVE-2020-12519**	https://cert.vde.com/en-us/advisories/vde-2020-049	O-PHO-PLCN-040121/908
Improper Input Validation	17-Dec-20	6.1	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	https://cert.vde.com/en-us/advisories/vde-2020-049	O-PHO-PLCN-040121/909
tc_mguard_rs4000_4g_vzw_vpn_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get	https://cert.vde.com/en-	O-PHO-TC_M-040121/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	us/advisories/vde-2020-046	
tc_mguard_rs4000_4g_att_vpn_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-TC_M-040121/911
fl_mguard_rs4004_tx\/dtx_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration.	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-FL_M-040121/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**		
fl_mguard_rs4004_tx\/dtx_vpn_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-FL_M-040121/913
tc_mguard_rs4000_3g_vpn_firmware					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch	https://cert.vde.com/en-us/advisories/vde-2020-046	O-PHO-TC_M-040121/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**		
Qnap					
quts_hero					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	29-Dec-20	6.5	This command injection vulnerability allows attackers to execute arbitrary commands in a compromised application. QNAP have already fixed this vulnerability in the following versions of QTS and QuTS hero. **CVE ID : CVE-2020-25847**	https://www.qnap.com/en/security-advisory/qsa-20-20	O-QNA-QUTS-040121/915
qts					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	29-Dec-20	6.5	This command injection vulnerability allows attackers to execute arbitrary commands in a compromised application. QNAP have already fixed this vulnerability in the following versions of QTS and QuTS hero. **CVE ID : CVE-2020-25847**	https://www.qnap.com/en/security-advisory/qsa-20-20	O-QNA-QTS-040121/916
Redhat					
enterprise_linux					
Misinterpretation of Input	21-Dec-20	10	A signature verification vulnerability exists in crewjam/saml. This flaw allows an attacker to	N/A	O-RED-ENTE-040121/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass SAML Authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. **CVE ID : CVE-2020-27846**		
Tendacn					
ac1200_firmware					
N/A	28-Dec-20	6.5	On Tenda AC1200 (Model AC6) 15.03.06.51_multi devices, admin, support, user, and nobody have a password of 1234. **CVE ID : CVE-2020-28093**	N/A	O-TEN-AC12-040121/918
N/A	28-Dec-20	5	On Tenda AC1200 (Model AC6) 15.03.06.51_multi devices, the default settings for the router speed test contain links to download malware named elive or CNKI E-Learning. **CVE ID : CVE-2020-28094**	N/A	O-TEN-AC12-040121/919
terra-master					
tos					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Dec-20	3.5	Cross-site scripting (XSS) vulnerability in TerraMaster TOS <= 4.2.06 allows remote authenticated users to inject arbitrary web script or HTML via the mod parameter to /module/index.php. **CVE ID : CVE-2020-28184**	N/A	O-TER-TOS-040121/920
N/A	24-Dec-20	5	User Enumeration vulnerability in	N/A	O-TER-TOS-040121/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TerraMaster TOS <= 4.2.06 allows remote unauthenticated attackers to identify valid users within the system via the username parameter to wizard/initialise.php. **CVE ID : CVE-2020-28185**		
Weak Password Recovery Mechanism for Forgotten Password	24-Dec-20	6.8	Email Injection in TerraMaster TOS <= 4.2.06 allows remote unauthenticated attackers to abuse the forget password functionality and achieve account takeover. **CVE ID : CVE-2020-28186**	N/A	O-TER-TOS-040121/922
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Dec-20	10	Multiple directory traversal vulnerabilities in TerraMaster TOS <= 4.2.06 allow remote authenticated attackers to read, edit or delete any file within the filesystem via the (1) filename parameter to /tos/index.php?editor/fileGet, Event parameter to /include/ajax/logtable.php , or opt parameter to /include/core/index.php. **CVE ID : CVE-2020-28187**	N/A	O-TER-TOS-040121/923
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Dec-20	10	Remote Command Execution (RCE) vulnerability in TerraMaster TOS <= 4.2.06 allow remote unauthenticated attackers to inject OS commands via /include/makecvs.php in Event parameter.	N/A	O-TER-TOS-040121/924

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-28188		
N/A	24-Dec-20	4.3	TerraMaster TOS <= 4.2.06 was found to check for updates (of both system and applications) via an insecure channel (HTTP). Man-in-the-middle attackers are able to intercept these requests and serve a weaponized/infected version of applications or updates. **CVE ID : CVE-2020-28190**	N/A	O-TER-TOS-040121/925
Incorrect Authorization	24-Dec-20	5.5	Incorrect Access Control vulnerability in TerraMaster TOS <= 4.2.06 allows remote authenticated attackers to bypass read-only restriction and obtain full access to any folder within the NAS **CVE ID : CVE-2020-29189**	N/A	O-TER-TOS-040121/926
terramaster_operating_system					
Unrestricted Upload of File with Dangerous Type	23-Dec-20	10	An unauthenticated command-execution vulnerability exists in TerraMaster TOS through 4.2.06 via shell metacharacters in the Event parameter in include/makecvs.php during CSV creation. **CVE ID : CVE-2020-35665**	N/A	O-TER-TERR-040121/927
Tp-link					
wa901nd_firmware					
Insufficiently	26-Dec-20	7.5	A password-disclosure	N/A	O-TP--WA90-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		040121/928
archer_c5_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N,	N/A	O-TP--ARCH-040121/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
archer_c7_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--ARCH-040121/930
mr3420_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative	N/A	O-TP--MR34-040121/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
mr6400_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N,	N/A	O-TP--MR64-040121/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wa701nd_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WA70-040121/933
wa801nd_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and	N/A	O-TP--WA80-040121/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wdr3500_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WDR3-040121/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wdr3600_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WDR3-040121/936
we843n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND,	N/A	O-TP--WE84-040121/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr1043nd_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR10-040121/938
wr1045nd_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices	N/A	O-TP--WR10-040121/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr740n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N,	N/A	O-TP--WR74-040121/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr741nd_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR74-040121/941
wr749n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND	N/A	O-TP--WR74-040121/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr802n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300	N/A	O-TP--WR80-040121/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. **CVE ID : CVE-2020-35575**		
wr840n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR84-040121/944
wr841hp_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400,	N/A	O-TP--WR84-040121/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr841n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR84-040121/946
wr842n_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR84-040121/947
wr842nd_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N,	N/A	O-TP--WR84-040121/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr845n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR84-040121/949
wr940n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to	N/A	O-TP--WR94-040121/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr941hp_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND,	N/A	O-TP--WR94-040121/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr945n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	O-TP--WR94-040121/952
wr949n_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before	N/A	O-TP--WR94-040121/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wrd4300_firmware					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices.	N/A	O-TP--WRD4-040121/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35575		
Vmware					
esxi					
NULL Pointer Dereference	21-Dec-20	2.1	VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition. **CVE ID : CVE-2020-3999**	N/A	O-VMW-ESXI-040121/955
Wago					
touch_panel_600_standard_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx)	https://cert.vde.com/en-us/advisories/vde-2020-045	O-WAG-TOUC-040121/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
touch_panel_600_advanced_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	O-WAG-TOUC-040121/957
touch_panel_600_marine_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions	https://cert.vde.com/en-us/advisories/vde-2020-045	O-WAG-TOUC-040121/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<=FW10. **CVE ID : CVE-2020-12522**		
pfc_200_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	O-WAG-PFC_-040121/959
pfc_100_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10.	https://cert.vde.com/en-us/advisories/vde-2020-045	O-WAG-PFC_-040121/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12522		
ZTE					
zxhn_e8810_firmware					
Origin Validation Error	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6881**	N/A	O-ZTE-ZXHN-040121/961
Insufficiently Protected Credentials	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26,	N/A	O-ZTE-ZXHN-040121/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6882**		
zxhn_e8820_firmware					
Origin Validation Error	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6881**	N/A	O-ZTE-ZXHN-040121/963
Insufficiently Protected Credentials	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN	N/A	O-ZTE-ZXHN-040121/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6882**		
zxhn_e8822_firmware					
Origin Validation Error	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6881**	N/A	O-ZTE-ZXHN-040121/965
Insufficiently Protected Credentials	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other	N/A	O-ZTE-ZXHN-040121/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6882**		
Zyxel					
usg1100_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG1-040121/967
usg110_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG1-040121/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
usg1900_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG1-040121/969
usg20-vpn_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG2-040121/970
usg20w-vpn_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware.	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://ww	O-ZYX-USG2-040121/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	w.zyxel.com/support/CVE-2020-29583.shtml	
usg210_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG2-040121/972
usg310_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG3-040121/973
usg40_firmware					
Cleartext Storage of	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains	http://ftp.zyxel.com/U	O-ZYX-USG4-040121/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	SG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	
usg40w_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG4-040121/975
usg60_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-	O-ZYX-USG6-040121/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with admin privileges. **CVE ID : CVE-2020-29583**	29583.shtml	
usg60w_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG6-040121/977
usg2200_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-USG2-040121/978
zywall110_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.p	O-ZYX-ZYWA-040121/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	df, https://www.zyxel.com/support/CVE-2020-29583.shtml	
zywall310_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-ZYWA-040121/980
zywall1100_firmware					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	O-ZYX-ZYWA-040121/981
Hardware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dell					
idrac9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	4.3	Dell EMC iDRAC9 versions prior to 4.32.10.00 and 4.40.00.00 contain a reflected cross-site scripting vulnerability in the iDRAC9 web application. A remote attacker could potentially exploit this vulnerability to run malicious HTML or JavaScript in a victim's browser by tricking a victim in to following a specially crafted link. **CVE ID : CVE-2020-26198**	N/A	H-DEL-IDRA-040121/982
D-link					
dsl2888a					
Incorrect Permission Assignment for Critical Resource	22-Dec-20	3.3	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It has a misconfigured FTP service that allows a malicious network user to access system folders and download sensitive files (such as the password hash file). **CVE ID : CVE-2020-24578**	https://www.trustwave.com/en-us/resources/security-resources/security-advisories/	H-D-L-DSL2-040121/983
Improper Authentication	22-Dec-20	5.8	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. An unauthenticated attacker could bypass authentication to access	https://www.trustwave.com/en-us/resources/security-resources/	H-D-L-DSL2-040121/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated pages and functionality. **CVE ID : CVE-2020-24579**	security-advisories/	
Improper Authentication	22-Dec-20	5.4	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. Lack of authentication functionality allows an attacker to assign a static IP address that was once used by a valid user. **CVE ID : CVE-2020-24580**	https://www.trustwave.com/en-us/resources/security-resources/security-advisories/	H-D-L-DSL2-040121/985
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Dec-20	7.7	An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It contains an execute_cmd.cgi feature (that is not reachable via the web user interface) that lets an authenticated user execute Operating System commands. **CVE ID : CVE-2020-24581**	https://www.trustwave.com/en-us/resources/security-resources/security-advisories/	H-D-L-DSL2-040121/986
Emerson					
x-stream_enhanced_xegp					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to	N/A	H-EME-X-ST-040121/987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain access to sensitive information. **CVE ID : CVE-2020-27254**		
x-stream_enhanced_xegk					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**	N/A	H-EME-X-ST-040121/988
x-stream_enhanced_xefd					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**	N/A	H-EME-X-ST-040121/989
x-stream_enhanced_xexf					
Improper Authentication	21-Dec-20	5	Emerson Rosemount X-STREAM Gas AnalyzerX-STREAM enhanced XEGP, XEGK, XEFD, XEXF – all	N/A	H-EME-X-ST-040121/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			revisions, The affected products are vulnerable to improper authentication for accessing log and backup data, which could allow an attacker with a specially crafted URL to obtain access to sensitive information. **CVE ID : CVE-2020-27254**		
Epson					
eps_tse_server_8					
Insufficiently Protected Credentials	16-Dec-20	7.5	Unrestricted access to the log downloader functionality in EPSON EPS TSE Server 8 (21.0.11) allows an unauthenticated attacker to remotely retrieve administrative hashed credentials via the maintenance/troubleshoot.php?download=1 URI. **CVE ID : CVE-2020-28929**	N/A	H-EPS-EPS_-040121/991
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-20	3.5	A Cross-Site Scripting (XSS) issue in the 'update user' and 'delete user' functionalities in settings/users.php in EPSON EPS TSE Server 8 (21.0.11) allows an authenticated attacker to inject a JavaScript payload in the user management page that is executed by an administrator. **CVE ID : CVE-2020-28930**	N/A	H-EPS-EPS_-040121/992
Cross-Site Request	16-Dec-20	6.8	Lack of an anti-CSRF token in the entire administrative	N/A	H-EPS-EPS_-040121/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			interface in EPSON EPS TSE Server 8 (21.0.11) allows an unauthenticated attacker to force an administrator to execute external POST requests by visiting a malicious website. **CVE ID : CVE-2020-28931**		
foscammall					
foscam_x1					
N/A	28-Dec-20	7.2	FOSCAM FHD X1 1.14.2.4 devices allow attackers (with physical UART access) to login via the ipc.fos~ password. **CVE ID : CVE-2020-28096**	N/A	H-FOS-FOSC-040121/994
HP					
storeever_msl2024					
Cross-Site Request Forgery (CSRF)	18-Dec-20	6.8	A potential security vulnerability has been identified in the HPE StoreEver MSL2024 Tape Library and HPE StoreEver 1/8 G2 Tape Autoloaders. The vulnerability could be remotely exploited to allow Cross-site Request Forgery (CSRF). **CVE ID : CVE-2020-7201**	N/A	H-HP-STOR-040121/995
storeever_1\/8_g2_tape_autoloader					
Cross-Site Request Forgery (CSRF)	18-Dec-20	6.8	A potential security vulnerability has been identified in the HPE StoreEver MSL2024 Tape Library and HPE StoreEver 1/8 G2 Tape Autoloaders.	N/A	H-HP-STOR-040121/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability could be remotely exploited to allow Cross-site Request Forgery (CSRF). **CVE ID : CVE-2020-7201**		
Huawei					
honor_20_pro					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-03-smartphone-en	H-HUA-HONO-040121/997
cloudengine_6800					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	H-HUA-CLOU-040121/998
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-	H-HUA-CLOU-040121/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	cloudengine-en	
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**	N/A	H-HUA-CLOU-040121/1000
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	H-HUA-CLOU-040121/1001
mate_30_pro					
Improper	24-Dec-20	4.6	There is a privilege	N/A	H-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**		MATE-040121/1002
cloudengine_5800					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	H-HUA-CLOU-040121/1003
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-cloudengine-en	H-HUA-CLOU-040121/1004
Improper Input	24-Dec-20	4.6	There is a privilege escalation vulnerability in	N/A	H-HUA-CLOU-040121/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**		
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	H-HUA-CLOU-040121/1006
cloudengine_7800					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	H-HUA-CLOU-040121/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to denial of service. **CVE ID : CVE-2020-9094**		
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-cloudengine-en	H-HUA-CLOU-040121/1008
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800. Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**	N/A	H-HUA-CLOU-040121/1009
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-	H-HUA-CLOU-040121/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	01-vrp-en	
jackman-al00d					
Uncontrolled Resource Consumption	29-Dec-20	2.1	There is a resource management error vulnerability in Jackman-AL00D versions 8.2.0.185(C00R2P1). Local attackers construct malicious application files, causing system applications to run abnormally. **CVE ID : CVE-2020-1848**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-02-smartphone-en	H-HUA-JACK-040121/1011
yale-l21a					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-03-smartphone-en	H-HUA-YALE-040121/1012
yale-l61a					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal	https://www.huawei.com/en/psirt/security-advisories/	H-HUA-YALE-040121/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	huawei-sa-20201216-03-smartphone-en	
p40					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**	N/A	H-HUA-P40-040121/1014
p40_pro					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**	N/A	H-HUA-P40_-040121/1015
princeton-al10d					
N/A	29-Dec-20	5	There is a denial of service vulnerability in some Huawei smartphones. Due to the improper processing of received abnormal	https://www.huawei.com/en/psirt/security-advisories/	H-HUA-PRIN-040121/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages, remote attackers may exploit this vulnerability to cause a denial of service (DoS) on the specific module. **CVE ID : CVE-2020-9223**	huawei-sa-20201216-03-smartphone-en	
cloudengine_12800					
Out-of-bounds Read	29-Dec-20	5	There is an out of bound read vulnerability in some verisons of Huawei CloudEngine product. A module does not deal with specific message properly. Attackers can exploit this vulnerability by sending malicious packet. This can lead to denial of service. **CVE ID : CVE-2020-9094**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-obr-en	H-HUA-CLOU-040121/1017
Allocation of Resources Without Limits or Throttling	29-Dec-20	5	There is a memory leak vulnerability in some versions of Huawei CloudEngine product. An unauthenticated, remote attacker may exploit this vulnerability by sending specific message to the affected product. Due to not release the allocated memory properly, successful exploit may cause memory leak. **CVE ID : CVE-2020-9124**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201223-01-cloudengine-en	H-HUA-CLOU-040121/1018
Improper Input Validation	24-Dec-20	4.6	There is a privilege escalation vulnerability in some versions of CloudEngine 12800,CloudEngine 5800,CloudEngine 6800 and CloudEngine 7800.	N/A	H-HUA-CLOU-040121/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Due to insufficient input validation, a local attacker with high privilege may execute some specially crafted scripts in the affected products. Successful exploit will cause privilege escalation. **CVE ID : CVE-2020-9137**		
Improper Authentication	29-Dec-20	6.8	There is an improper authentication vulnerability in some verisons of Huawei CloudEngine product. A module does not verify the input file properly. Attackers can exploit this vulnerability by crafting malicious files to bypass current verification mechanism. This can compromise normal service. **CVE ID : CVE-2020-9207**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-vrp-en	H-HUA-CLOU-040121/1020
nip6800					
Out-of-bounds Read	24-Dec-20	3.3	There is an out-of-bounds read vulnerability in some versions of NIP6800, Secospace USG6600 and USG9500. The software reads data past the end of the intended buffer when parsing DHCP messages including crafted parameter. Successful exploit could cause certain service abnormal. **CVE ID : CVE-2020-9201**	N/A	H-HUA-NIP6-040121/1021
secospace_usg6600					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-Dec-20	3.3	There is an out-of-bounds read vulnerability in some versions of NIP6800, Secospace USG6600 and USG9500. The software reads data past the end of the intended buffer when parsing DHCP messages including crafted parameter. Successful exploit could cause certain service abnormal. **CVE ID : CVE-2020-9201**	N/A	H-HUA-SECO-040121/1022
taurus-al00a					
Use After Free	29-Dec-20	4.3	There is a use after free vulnerability in Taurus-AL00A versions 10.0.0.1(C00E1R1P1). A module does not deal with specific message properly, which makes a function refer to memory after it has been freed. Attackers can exploit this vulnerability by running a crafted application with common privilege. This would compromise normal service. **CVE ID : CVE-2020-9093**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-smartphone-en	H-HUA-TAUR-040121/1023
mate_10					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and	N/A	H-HUA-MATE-040121/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**		
mate_30					
Improper Privilege Management	24-Dec-20	4.6	There is a privilege escalation vulnerability on some Huawei smart phones due to design defects. The attacker needs to physically contact the mobile phone and obtain higher privileges, and execute relevant commands, resulting in the user's privilege promotion. **CVE ID : CVE-2020-9119**	N/A	H-HUA-MATE-040121/1025
Out-of-bounds Read	29-Dec-20	4.6	There is an out-of-bound read vulnerability in huawei smartphone Mate 30 versions earlier than 10.1.0.156 (C00E155R7P2). An attacker with specific permission can exploit this vulnerability by sending crafted packet with specific parameter to the target device. Due to insufficient validation of the parameter, successful exploit can cause the device to behave abnormally. **CVE ID : CVE-2020-9125**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20201216-01-taurus-en	H-HUA-MATE-040121/1026
usg9500					
Out-of-bounds Read	24-Dec-20	3.3	There is an out-of-bounds read vulnerability in some	N/A	H-HUA-USG9-040121/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions of NIP6800, Secospace USG6600 and USG9500. The software reads data past the end of the intended buffer when parsing DHCP messages including crafted parameter. Successful exploit could cause certain service abnormal. **CVE ID : CVE-2020-9201**		
kyland					
kps2204_6_port_managed_din-rail_programmable_serial_device					
Unrestricted Upload of File with Dangerous Type	17-Dec-20	7.5	An arbitrary code execution vulnerability in Kyland KPS2204 6 Port Managed Din-Rail Programmable Serial Device Servers Software Version:R0002.P05 allows remote attackers to upload a malicious script file by constructing a POST type request and writing a payload in the request parameters as an instruction to write a file. **CVE ID : CVE-2020-25010**	N/A	H-KYL-KPS2-040121/1028
Insufficiently Protected Credentials	17-Dec-20	5	A sensitive information disclosure vulnerability in Kyland KPS2204 6 Port Managed Din-Rail Programmable Serial Device Servers Software Version:R0002.P05 allows remote attackers to get username and password by request /cgi-bin/webadminget.cgi	N/A	H-KYL-KPS2-040121/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			script via the browser. **CVE ID : CVE-2020-25011**		
Lantronix					
xport_edge					
Improper Authentication	18-Dec-20	4	An authentication bypass vulnerability exists in the Web Manager functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause increased privileges. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-13527**	N/A	H-LAN-XPOR-040121/1030
Cleartext Transmission of Sensitive Information	18-Dec-20	4.3	An information disclosure vulnerability exists in the Web Manager and telnet CLI functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A specially crafted HTTP request can cause information disclosure. An attacker can sniff the network to trigger this vulnerability. **CVE ID : CVE-2020-13528**	N/A	H-LAN-XPOR-040121/1031
sgx					
Improper Authentication	18-Dec-20	4	An authentication bypass vulnerability exists in the Web Manager functionality of Lantronix XPort EDGE 3.0.0.0R11, 3.1.0.0R9, 3.4.0.0R12 and 4.2.0.0R7. A	N/A	H-LAN-SGX-040121/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted HTTP request can cause increased privileges. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-13527**		
Linksys					
re6500					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-20	10	Belkin LINKSYS RE6500 devices before 1.0.012.001 allow remote attackers to execute arbitrary commands or set a new password via shell metacharacters to the goform/setSysAdm page. **CVE ID : CVE-2020-35713**	N/A	H-LIN-RE65-040121/1033
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Dec-20	6.5	Belkin LINKSYS RE6500 devices before 1.0.11.001 allow remote authenticated users to execute arbitrary commands via goform/systemCommand?command= in conjunction with the goform/pingstart program. **CVE ID : CVE-2020-35714**	N/A	H-LIN-RE65-040121/1034
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-20	9	Belkin LINKSYS RE6500 devices before 1.0.012.001 allow remote authenticated users to execute arbitrary commands via shell metacharacters in a filename to the upload_settings.cgi page. **CVE ID : CVE-2020-35715**	N/A	H-LIN-RE65-040121/1035
N/A	26-Dec-20	7.8	Belkin LINKSYS RE6500	N/A	H-LIN-RE65-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices before 1.0.012.001 allow remote attackers to cause a persistent denial of service (segmentation fault) via a long /goform/langSwitch langSelectionOnly parameter. **CVE ID : CVE-2020-35716**		040121/1036
mersive					
solstice_pod					
N/A	23-Dec-20	4.3	In Solstice Pod before 3.0.3, the web services allow users to connect to them over unencrypted channels via the Browser Look-in feature. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the web services and obtain any information the user supplies, including Administrator passwords and screen keys. **CVE ID : CVE-2020-35584**	N/A	H-MER-SOLS-040121/1037
Improper Restriction of Excessive Authentication Attempts	23-Dec-20	5	In Solstice Pod before 3.3.0 (or Open4.3), the screen key can be enumerated using brute-force attacks via the /lookin/info Solstice Open Control API because there are only 1.7 million possibilities. **CVE ID : CVE-2020-35585**	N/A	H-MER-SOLS-040121/1038
Improper Restriction of	23-Dec-20	5	In Solstice Pod before 3.3.0 (or Open4.3), the	N/A	H-MER-SOLS-040121/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Excessive Authentication Attempts			Administrator password can be enumerated using brute-force attacks via the /Config/service/initModel?password= Solstice Open Control API because there is no complexity requirement (e.g., it might be all digits or all lowercase letters). **CVE ID : CVE-2020-35586**		
solstice					
N/A	23-Dec-20	5	** DISPUTED ** In Solstice Pod before 3.0.3, the firmware can easily be decompiled/disassembled. The decompiled/disassembled files contain non-obfuscated code. NOTE: it is unclear whether lack of obfuscation is directly associated with a negative impact, or instead only facilitates an attack technique. **CVE ID : CVE-2020-35587**	N/A	H-MER-SOLS-040121/1040
Mitel					
6873i_sip					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection,	N/A	H-MIT-6873-040121/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27639**		
6930_sip					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27639**	N/A	H-MIT-6930-040121/1042
6940_sip					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6873i, 6930, and 6940 SIP phones with firmware before 5.1.0.SP6 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations.	N/A	H-MIT-6940-040121/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27639		
mivoice_6940					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6940 and 6930 MiNet phones with firmware before 1.5.3 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27640**	N/A	H-MIT-MIVO-040121/1044
mivoice_6930					
N/A	18-Dec-20	4.8	The Bluetooth handset of Mitel MiVoice 6940 and 6930 MiNet phones with firmware before 1.5.3 could allow an unauthenticated attacker within Bluetooth range to pair a rogue Bluetooth device when a phone handset loses connection, due to an improper pairing mechanism. A successful exploit could allow an attacker to eavesdrop on conversations. **CVE ID : CVE-2020-27640**	N/A	H-MIT-MIVO-040121/1045
Moxa					
nport_iaw5000a-i\/o					
Weak	23-Dec-20	5	The built-in web service for	N/A	H-MOX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Password Requirements			MOXA NPort IAW5000A-I/O firmware version 2.1 or lower does not require users to have strong passwords. **CVE ID : CVE-2020-25153**		NPOR-040121/1046
Cleartext Transmission of Sensitive Information	23-Dec-20	5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower stores and transmits the credentials of third-party services in cleartext. **CVE ID : CVE-2020-25190**	N/A	H-MOX-NPOR-040121/1047
Information Exposure	23-Dec-20	5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower allows sensitive information to be displayed without proper authorization. **CVE ID : CVE-2020-25192**	N/A	H-MOX-NPOR-040121/1048
Improper Privilege Management	23-Dec-20	6.5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower has improper privilege management, which may allow an attacker with user privileges to perform requests with administrative privileges. **CVE ID : CVE-2020-25194**	N/A	H-MOX-NPOR-040121/1049
Improper Restriction of Excessive Authentication Attempts	23-Dec-20	5	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower allows SSH/Telnet sessions, which may be vulnerable to brute force	N/A	H-MOX-NPOR-040121/1050

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks to bypass authentication. **CVE ID : CVE-2020-25196**		
Session Fixation	23-Dec-20	6.8	The built-in WEB server for MOXA NPort IAW5000A-I/O firmware version 2.1 or lower has incorrectly implemented protections from session fixation, which may allow an attacker to gain access to a session and hijack it by stealing the user's cookies. **CVE ID : CVE-2020-25198**	N/A	H-MOX-NPOR-040121/1051
NEC					
m120					
Improper Certificate Validation	24-Dec-20	5.8	iSM client versions from V5.1 prior to V12.1 running on NEC Storage Manager or NEC Storage Manager Express does not verify a server certificate properly, which allows a man-in-the-middle attacker to eavesdrop on an encrypted communication or alter the communication via a crafted certificate. **CVE ID : CVE-2020-5684**	N/A	H-NEC-M120-040121/1052
m12e					
Improper Certificate Validation	24-Dec-20	5.8	iSM client versions from V5.1 prior to V12.1 running on NEC Storage Manager or NEC Storage Manager Express does not verify a server certificate properly, which allows a man-in-the-middle attacker to	N/A	H-NEC-M12E-040121/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			eavesdrop on an encrypted communication or alter the communication via a crafted certificate. **CVE ID : CVE-2020-5684**		
m320					
Improper Certificate Validation	24-Dec-20	5.8	iSM client versions from V5.1 prior to V12.1 running on NEC Storage Manager or NEC Storage Manager Express does not verify a server certificate properly, which allows a man-in-the-middle attacker to eavesdrop on an encrypted communication or alter the communication via a crafted certificate. **CVE ID : CVE-2020-5684**	N/A	H-NEC-M320-040121/1054
m320f					
Improper Certificate Validation	24-Dec-20	5.8	iSM client versions from V5.1 prior to V12.1 running on NEC Storage Manager or NEC Storage Manager Express does not verify a server certificate properly, which allows a man-in-the-middle attacker to eavesdrop on an encrypted communication or alter the communication via a crafted certificate. **CVE ID : CVE-2020-5684**	N/A	H-NEC-M320-040121/1055
Netgear					
rbs40					
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-RBS4-040121/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBS4-040121/1057
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-RBS4-040121/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-RBS4-040121/1059
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-RBS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		040121/1060
rbk40					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	H-NET-RBK4-040121/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	H-NET-RBK4-040121/1062
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-RBK4-040121/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBK4-040121/1064
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-RBK4-040121/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-RBK4-040121/1066
rbr50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before	N/A	H-NET-RBR5-040121/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-RBR5-040121/1068
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-RBR5-040121/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-RBR5-040121/1070
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-RBR5-040121/1071
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before	N/A	H-NET-RBR5-040121/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	H-NET-RBR5-040121/1073
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-RBR5-040121/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-RBR5-040121/1075
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before	N/A	H-NET-RBR5-040121/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-RBR5-040121/1077
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	H-NET-RBR5-040121/1078
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-RBR5-040121/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-RBR5-040121/1080
rbs50					
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	H-NET-RBS5-040121/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-RBS5-040121/1082
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before	N/A	H-NET-RBS5-040121/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-RBS5-040121/1084
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	H-NET-RBS5-040121/1085

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35820		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBS5-040121/1086
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	H-NET-RBS5-040121/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35805		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-RBS5-040121/1088
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-RBS5-040121/1089
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	H-NET-RBS5-040121/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-RBS5-040121/1091
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	H-NET-RBS5-040121/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	H-NET-RBS5-040121/1093
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-RBS5-040121/1094
rbk50					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	H-NET-RBK5-040121/1095
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	H-NET-RBK5-040121/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**	N/A	H-NET-RBK5-040121/1097
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-RBK5-040121/1098
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	H-NET-RBK5-040121/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBK5-040121/1100
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before	N/A	H-NET-RBK5-040121/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-RBK5-040121/1102
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-RBK5-040121/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	H-NET-RBK5-040121/1104
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-RBK5-040121/1105
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-RBK5-040121/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	H-NET-RBK5-040121/1107
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before	N/A	H-NET-RBK5-040121/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
r6220					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-R622-040121/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	H-NET-R622-040121/1110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-R622-040121/1111
r6260					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-R626-040121/1112
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before	N/A	H-NET-R626-040121/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-R626-040121/1114
r6800					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before	N/A	H-NET-R680-040121/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
d7000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before	N/A	H-NET-D700-040121/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050	N/A	H-NET-D700-040121/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-D700-040121/1118
d6200					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before	N/A	H-NET-D620-040121/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	H-NET-D620-040121/1120
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before	N/A	H-NET-D620-040121/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
pr2000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before	N/A	H-NET-PR20-040121/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r6050					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before	N/A	H-NET-R605-040121/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**	N/A	H-NET-R605-040121/1124
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before	N/A	H-NET-R605-040121/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**		
jr6150					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-JR61-040121/1126
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-JR61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		040121/1127
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-JR61-040121/1128
r6120					
Buffer Copy	30-Dec-20	5.2	Certain NETGEAR devices	N/A	H-NET-R612-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		040121/1129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5	N/A	H-NET-R612-040121/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-R612-040121/1131
jgs516pe					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48,	N/A	H-NET-JGS5-040121/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**		
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**	N/A	H-NET-JGS5-040121/1133
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	H-NET-JGS5-040121/1134
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**	N/A	H-NET-JGS5-040121/1135
rbk752					
Improper Neutralization of Special Elements used	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This	N/A	H-NET-RBK7-040121/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in a Command ('Command Injection')			affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**		
rbr750					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	H-NET-RBR7-040121/1137
rbs750					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	H-NET-RBS7-040121/1138
rbk852					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	H-NET-RBK8-040121/1139
rbr850					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	H-NET-RBR8-040121/1140
rbs850					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	N/A	H-NET-RBS8-040121/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-35794**		
r6020					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-R602-040121/1142
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	H-NET-R602-040121/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-R602-040121/1144
r6080					
Buffer Copy without	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer	N/A	H-NET-R608-040121/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	H-NET-R608-040121/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-R608-040121/1147
wnr2020					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020	N/A	H-NET-WNR2-040121/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-WNR2-040121/1149
r7500v2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	H-NET-R750-040121/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-R750-040121/1151
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	H-NET-R750-040121/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-R750-040121/1153
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-R750-040121/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	H-NET-R750-040121/1155
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-R750-040121/1156
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before	N/A	H-NET-R750-040121/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	H-NET-R750-040121/1158
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	H-NET-R750-040121/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	H-NET-R750-040121/1160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	H-NET-R750-040121/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	H-NET-R750-040121/1162
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	H-NET-R750-040121/1163
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-R750-040121/1164

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ex7000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-EX70-040121/1165
gs716t					
Cross-Site Request Forgery (CSRF)	30-Dec-20	6.8	Certain NETGEAR devices are affected by CSRF. This affects GS716Tv3 before 6.3.1.36 and GS724Tv4	N/A	H-NET-GS71-040121/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 6.3.1.36. **CVE ID : CVE-2020-35778**		
gs724t					
Cross-Site Request Forgery (CSRF)	30-Dec-20	6.8	Certain NETGEAR devices are affected by CSRF. This affects GS716Tv3 before 6.3.1.36 and GS724Tv4 before 6.3.1.36. **CVE ID : CVE-2020-35778**	N/A	H-NET-GS72-040121/1167
r7000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before	N/A	H-NET-R700-040121/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
dgn2200					
Improper Authentication	30-Dec-20	5.8	NETGEAR DGN2200v1 devices before v1.0.0.60 mishandle HTTPd authentication (aka PSV-2020-0363, PSV-2020-0364, and PSV-2020-0365). **CVE ID : CVE-2020-35785**	N/A	H-NET-DGN2-040121/1169
r6300					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before	N/A	H-NET-R630-040121/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r6700					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before	N/A	H-NET-R670-040121/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
r6900p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-R690-040121/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
r6900					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-R690-040121/1173
r7000p					
Buffer Copy without Checking Size of Input	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This	N/A	H-NET-R700-040121/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
dgn2200v1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	7.7	NETGEAR DGN2200v1 devices before v1.0.0.58 are affected by command injection. **CVE ID : CVE-2020-35777**	N/A	H-NET-DGN2-040121/1175
nms300					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Dec-20	7.8	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service. **CVE ID : CVE-2020-35779**	N/A	H-NET-NMS3-040121/1176
N/A	30-Dec-20	4	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service. **CVE ID : CVE-2020-35780**	N/A	H-NET-NMS3-040121/1177
N/A	30-Dec-20	4	NETGEAR NMS300 devices before 1.6.0.27 are affected by denial of service. **CVE ID : CVE-2020-35781**	N/A	H-NET-NMS3-040121/1178
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	6.5	NETGEAR NMS300 devices before 1.6.0.27 are affected by command injection by an authenticated user. **CVE ID : CVE-2020-35789**	N/A	H-NET-NMS3-040121/1179
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	7.5	NETGEAR NMS300 devices before 1.6.0.27 are affected by command injection by an unauthenticated attacker. **CVE ID : CVE-2020-35797**	N/A	H-NET-NMS3-040121/1180
d7800					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before	N/A	H-NET-D780-040121/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-D780-040121/1182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before	N/A	H-NET-D780-040121/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-D780-040121/1184
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-D780-040121/1185
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-D780-040121/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	H-NET-D780-040121/1187
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26. **CVE ID : CVE-2020-35790**	N/A	H-NET-D780-040121/1188
Improper	30-Dec-20	4.6	Certain NETGEAR devices	N/A	H-NET-D780-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**		040121/1189
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**	N/A	H-NET-D780-040121/1190
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	H-NET-D780-040121/1191

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35805		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-D780-040121/1192
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-D780-040121/1193
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	H-NET-D780-040121/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-D780-040121/1195
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	H-NET-D780-040121/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	H-NET-D780-040121/1197
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-D780-040121/1198
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-D780-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**		040121/1199
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	H-NET-D780-040121/1200
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-D780-040121/1201
r7500					
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-R750-040121/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**	N/A	H-NET-R750-040121/1203
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	H-NET-R750-040121/1204
r7800					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	H-NET-R780-040121/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-R780-040121/1206
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	H-NET-R780-040121/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-R780-040121/1208
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-R780-040121/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-R780-040121/1210
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	H-NET-R780-040121/1211
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	2.7	NETGEAR R7800 devices before 1.0.2.74 are affected by a buffer overflow by an authenticated user. **CVE ID : CVE-2020-35786**	N/A	H-NET-R780-040121/1212
Buffer Copy without	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer	N/A	H-NET-R780-040121/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before	N/A	H-NET-R780-040121/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.26. **CVE ID : CVE-2020-35790**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35791**	N/A	H-NET-R780-040121/1215
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**	N/A	H-NET-R780-040121/1216
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	H-NET-R780-040121/1217
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before	N/A	H-NET-R780-040121/1218

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	H-NET-R780-040121/1219
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-R780-040121/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-R780-040121/1221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	H-NET-R780-040121/1222
Improper Neutralization of Input During Web Page	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before	N/A	H-NET-R780-040121/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	H-NET-R780-040121/1224
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78.	N/A	H-NET-R780-040121/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35827		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-R780-040121/1226
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	H-NET-R780-040121/1227
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-R780-040121/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-R780-040121/1229
r8900					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before	N/A	H-NET-R890-040121/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26. **CVE ID : CVE-2020-35790**	N/A	H-NET-R890-040121/1231
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35791**	N/A	H-NET-R890-040121/1232
Improper Neutralization of Special Elements used in a Command	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before	N/A	H-NET-R890-040121/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	H-NET-R890-040121/1234
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**	N/A	H-NET-R890-040121/1235
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before	N/A	H-NET-R890-040121/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-R890-040121/1237
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-R890-040121/1238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-R890-040121/1239
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	H-NET-R890-040121/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35817		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-R890-040121/1241
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-R890-040121/1242
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before	N/A	H-NET-R890-040121/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	H-NET-R890-040121/1244
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-R890-040121/1245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	H-NET-R890-040121/1246
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-R890-040121/1247
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-R890-040121/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	H-NET-R890-040121/1249
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before	N/A	H-NET-R890-040121/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	H-NET-R890-040121/1251
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	H-NET-R890-040121/1252
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before	N/A	H-NET-R890-040121/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35838**		
r9000					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	H-NET-R900-040121/1254
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before	N/A	H-NET-R900-040121/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**	N/A	H-NET-R900-040121/1256
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-R900-040121/1257
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-R900-040121/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-R900-040121/1259
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before	N/A	H-NET-R900-040121/1260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-R900-040121/1261
Improper Neutralization of Special	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an	N/A	H-NET-R900-040121/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			authenticated user. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, and R9000 before 1.0.4.26. **CVE ID : CVE-2020-35790**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7800 before 1.0.2.68, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35791**	N/A	H-NET-R900-040121/1263
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7500v2 before 1.0.3.48, R8900 before 1.0.5.2, R9000 before 1.0.5.2, and R7800 before 1.0.2.68. **CVE ID : CVE-2020-35792**	N/A	H-NET-R900-040121/1264
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	4.6	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.2, and R9000 before 1.0.5.2. **CVE ID : CVE-2020-35793**	N/A	H-NET-R900-040121/1265
Information	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure	N/A	H-NET-R900-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34. **CVE ID : CVE-2020-35804**		040121/1266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	H-NET-R900-040121/1267
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-R900-040121/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-R900-040121/1269
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	H-NET-R900-040121/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35824		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-R900-040121/1271
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	H-NET-R900-040121/1272
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before	N/A	H-NET-R900-040121/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-R900-040121/1274
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	H-NET-R900-040121/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	H-NET-R900-040121/1276
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-R900-040121/1277
rax120					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before	N/A	H-NET-RAX1-040121/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-RAX1-040121/1279
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	H-NET-RAX1-040121/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-RAX1-040121/1281
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-RAX1-040121/1282
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	H-NET-RAX1-040121/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	H-NET-RAX1-040121/1284
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before	N/A	H-NET-RAX1-040121/1285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-RAX1-040121/1286
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before	N/A	H-NET-RAX1-040121/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	H-NET-RAX1-040121/1288
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-RAX1-040121/1289
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	H-NET-RAX1-040121/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	H-NET-RAX1-040121/1291
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before	N/A	H-NET-RAX1-040121/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	H-NET-RAX1-040121/1293
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	H-NET-RAX1-040121/1294
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-RAX1-040121/1295

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xr500					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**	N/A	H-NET-XR50-040121/1296
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-XR50-040121/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-XR50-040121/1298
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before	N/A	H-NET-XR50-040121/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-XR50-040121/1300
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	H-NET-XR50-040121/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-XR50-040121/1302
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-XR50-040121/1303
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-XR50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**		040121/1304
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-XR50-040121/1305
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	H-NET-XR50-040121/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**	N/A	H-NET-XR50-040121/1307
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	H-NET-XR50-040121/1308
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	H-NET-XR50-040121/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-XR50-040121/1310
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	H-NET-XR50-040121/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**	N/A	H-NET-XR50-040121/1312
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-XR50-040121/1313
xr700					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before	N/A	H-NET-XR70-040121/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-XR70-040121/1315
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before	N/A	H-NET-XR70-040121/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35817**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35819**	N/A	H-NET-XR70-040121/1317
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35820**	N/A	H-NET-XR70-040121/1318
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-XR70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		040121/1319
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35822**	N/A	H-NET-XR70-040121/1320
Information Exposure	30-Dec-20	2.1	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7800 before 1.0.1.58, R7800 before 1.0.2.74, R8900 before 1.0.5.18, R9000 before 1.0.5.18, and XR700 before 1.0.1.34.	N/A	H-NET-XR70-040121/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35804		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	H-NET-XR70-040121/1322
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35809**	N/A	H-NET-XR70-040121/1323
Improper Neutralization	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS.	N/A	H-NET-XR70-040121/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35824**	N/A	H-NET-XR70-040121/1325
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before	N/A	H-NET-XR70-040121/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35825**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35826**	N/A	H-NET-XR70-040121/1327
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, XR500 before 2.3.2.56, XR700 before 1.0.1.10, and RAX120 before 1.0.0.78. **CVE ID : CVE-2020-35827**	N/A	H-NET-XR70-040121/1328
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-XR70-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		040121/1329
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35835**	N/A	H-NET-XR70-040121/1330
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before	N/A	H-NET-XR70-040121/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35837**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35838**	N/A	H-NET-XR70-040121/1332
rbr20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	H-NET-RBR2-040121/1333
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-RBR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		040121/1334
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBR2-040121/1335
Improper	30-Dec-20	3.5	Certain NETGEAR devices	N/A	H-NET-RBR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		040121/1336
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10.	N/A	H-NET-RBR2-040121/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35823		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-RBR2-040121/1338
rbs20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before	N/A	H-NET-RBS2-040121/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**	N/A	H-NET-RBS2-040121/1340
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before	N/A	H-NET-RBS2-040121/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBS2-040121/1342
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before	N/A	H-NET-RBS2-040121/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-RBS2-040121/1344
rbk20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before	N/A	H-NET-RBK2-040121/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35815**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**	N/A	H-NET-RBK2-040121/1346
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before	N/A	H-NET-RBK2-040121/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**	N/A	H-NET-RBK2-040121/1348
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before	N/A	H-NET-RBK2-040121/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**	N/A	H-NET-RBK2-040121/1350
rbr40					
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-RBR4-040121/1351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35816**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35821**	N/A	H-NET-RBR4-040121/1352
Improper Neutralization of Input During Web Page Generation	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before	N/A	H-NET-RBR4-040121/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35805**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35823**	N/A	H-NET-RBR4-040121/1354
Improper Neutralization of Input During	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before	N/A	H-NET-RBR4-040121/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0.1.56, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.4.28, R9000 before 1.0.4.28, RAX120 before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK50 before 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, XR500 before 2.3.2.56, and XR700 before 1.0.1.10. **CVE ID : CVE-2020-35830**		
jgs524e					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**	N/A	H-NET-JGS5-040121/1356
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**	N/A	H-NET-JGS5-040121/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	H-NET-JGS5-040121/1358
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**	N/A	H-NET-JGS5-040121/1359
jgs524pe					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**	N/A	H-NET-JGS5-040121/1360
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before	N/A	H-NET-JGS5-040121/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.6.0.48. **CVE ID : CVE-2020-35783**		
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	H-NET-JGS5-040121/1362
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**	N/A	H-NET-JGS5-040121/1363
gs116e					
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35782**	N/A	H-NET-GS11-040121/1364
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48,	N/A	H-NET-GS11-040121/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GS116Ev2 before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and JGS524PE before 2.6.0.48. **CVE ID : CVE-2020-35783**		
N/A	30-Dec-20	6.5	Certain NETGEAR devices are affected by lack of access control at the function level. This affects JGS516PE before 2.6.0.48, JGS524PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35784**	N/A	H-NET-GS11-040121/1366
N/A	30-Dec-20	5.8	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JGS516PE before 2.6.0.48, JGS524Ev2 before 2.6.0.48, JGS524PE before 2.6.0.48, and GS116Ev2 before 2.6.0.48. **CVE ID : CVE-2020-35801**	N/A	H-NET-GS11-040121/1367
d3600					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before	N/A	H-NET-D360-040121/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
d6000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before	N/A	H-NET-D600-040121/1369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
ex6200					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before	N/A	H-NET-EX62-040121/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
ex8000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before	N/A	H-NET-EX80-040121/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40. **CVE ID : CVE-2020-35787**		
wac104					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Dec-20	5.2	NETGEAR WAC104 devices before 1.0.4.13 are affected by a buffer overflow by an authenticated user. **CVE ID : CVE-2020-35788**	N/A	H-NET-WAC1-040121/1372
rbs40v					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	30-Dec-20	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS40V before 2.6.1.4, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-35794**	N/A	H-NET-RBS4-040121/1373
jnr1010v2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080	N/A	H-NET-JNR1-040121/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-JNR1-040121/1375
jwnr2010v5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080	N/A	H-NET-JWNR-040121/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-JWNR-040121/1377
wnr1000v4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080	N/A	H-NET-WNR1-040121/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-WNR1-040121/1379
wnr2050					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080	N/A	H-NET-WNR2-040121/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35840**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Dec-20	3.5	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1010v2 before 1.1.0.62, JR6150 before 1.0.1.24, JWNR2010v5 before 1.1.0.62, R6020 before 1.0.0.42, R6050 before 1.0.1.24, R6080 before 1.0.0.42, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6260 before 1.1.0.76, WNR1000v4 before 1.1.0.62, WNR2020 before 1.1.0.62, and WNR2050 before 1.1.0.62. **CVE ID : CVE-2020-35842**	N/A	H-NET-WNR2-040121/1381
Panasonic					
wv-s2231l					
Use of Hard-coded Credentials	28-Dec-20	2.1	Panasonic Security System WV-S2231L 4.25 has an insecure hard-coded password of lkjhgfdsa (which is just the asdf keyboard row in reverse order). **CVE ID : CVE-2020-29193**	N/A	H-PAN-WV-S-040121/1382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	28-Dec-20	5	Panasonic Security System WV-S2231L 4.25 allows a denial of service of the admin control panel (which will require a physical reset to restore administrative control) via Randomnum=99AC8CEC6E845B28&mode=1 in a POST request to the cgi-bin/set_factory URI. **CVE ID : CVE-2020-29194**	N/A	H-PAN-WV-S-040121/1383
Phoenixcontact					
tc_mguard_rs4000_4g_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-TC_M-040121/1384
innominate_mguard_rs4000_4tx\/tx					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-INNO-040121/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**		
innominate_mguard_rs4000_4tx\/tx_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-INNO-040121/1386
innominate_mguard_rs4000_4tx\/3g\/tx_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-INNO-040121/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**		
axc_f_2152					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1388
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks. **CVE ID : CVE-2020-12518**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1389
Improper Privilege Management	17-Dec-20	10	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges. **CVE ID : CVE-2020-12519**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1390
Improper	17-Dec-20	6.1	On Phoenix Contact	https://cer	H-PHO-AXC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	t.vde.com/en-us/advisories/vde-2020-049	040121/1391
axc_f_2152_starterkit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1392
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks. **CVE ID : CVE-2020-12518**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1393
Improper Privilege Management	17-Dec-20	10	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges.	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1394

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12519		
Improper Input Validation	17-Dec-20	6.1	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1395
axc_f_1152					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1396
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks. **CVE ID : CVE-2020-12518**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1397
Improper Privilege Management	17-Dec-20	10	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this	https://cert.vde.com/en-us/advisori	H-PHO-AXC_-040121/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability i.e. to open a reverse shell with root privileges. **CVE ID : CVE-2020-12519**	es/vde-2020-049	
Improper Input Validation	17-Dec-20	6.1	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1399
axc_f_3152					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1400
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks. **CVE ID : CVE-2020-12518**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1401
Improper	17-Dec-20	10	On Phoenix Contact	https://cer	H-PHO-AXC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges. **CVE ID : CVE-2020-12519**	t.vde.com/en-us/advisories/vde-2020-049	040121/1402
Improper Input Validation	17-Dec-20	6.1	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-AXC_-040121/1403
rfc_4072s					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-RFC_-040121/1404
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks.	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-RFC_-040121/1405

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12518		
Improper Privilege Management	17-Dec-20	10	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges. **CVE ID : CVE-2020-12519**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-RFC_-040121/1406
Improper Input Validation	17-Dec-20	6.1	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-RFC_-040121/1407
plcnext_technology_starterkit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-20	6	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation). **CVE ID : CVE-2020-12517**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-PLCN-040121/1408
Information Exposure	17-Dec-20	5	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use the knowledge gained by reading the insufficiently	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-PLCN-040121/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protected sensitive information to plan further attacks. **CVE ID : CVE-2020-12518**		
Improper Privilege Management	17-Dec-20	10	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an attacker can use this vulnerability i.e. to open a reverse shell with root privileges. **CVE ID : CVE-2020-12519**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-PLCN-040121/1410
Improper Input Validation	17-Dec-20	6.1	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS a specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot. **CVE ID : CVE-2020-12521**	https://cert.vde.com/en-us/advisories/vde-2020-049	H-PHO-PLCN-040121/1411
tc_mguard_rs4000_4g_vzw_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-TC_M-040121/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Initialization of Resource **CVE ID : CVE-2020-12523**		
tc_mguard_rs4000_4g_att_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-TC_M-040121/1413
fl_mguard_rs4004_tx\/dtx					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-FL_M-040121/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fl_mguard_rs4004_tx\/dtx_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-FL_M-040121/1415
tc_mguard_rs4000_3g_vpn					
Missing Initialization of Resource	17-Dec-20	6.4	On Phoenix Contact mGuard Devices versions before 8.8.3 LAN ports get functional after reboot even if they are disabled in the device configuration. For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource **CVE ID : CVE-2020-12523**	https://cert.vde.com/en-us/advisories/vde-2020-046	H-PHO-TC_M-040121/1416
Qualcomm					
sm8250					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Power Consumption	18-Dec-20	7.8	An issue was discovered on Samsung mobile devices with Q(10.0) and R(11.0) (Qualcomm SM8250 chipsets) software. They allows attackers to cause a denial of service (unlock failure) by triggering a power-shortage incident that causes a false-positive attack detection. The Samsung ID is SVE-2020-19678 (December 2020). **CVE ID : CVE-2020-35553**	N/A	H-QUA-SM82-040121/1417
Samsung					
galaxy_a3					
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable	N/A	H-SAM-GALA-040121/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
galaxy_note_4					
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly	N/A	H-SAM-GALA-040121/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
galaxy_note_5					
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as	N/A	H-SAM-GALA-040121/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
galaxy_s5					
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable	N/A	H-SAM-GALA-040121/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
j2_pro_\(2018\)					
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any	N/A	H-SAM-J2_P-040121/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
tab_a_\(2017\)					
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-	N/A	H-SAM-TAB_-040121/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy S5. **CVE ID : CVE-2020-35693**		
galaxy_s6_edge					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	24-Dec-20	5.4	On some Samsung phones and tablets running Android through 7.1.1, it is possible for an attacker-controlled Bluetooth Low Energy (BLE) device to pair silently with a vulnerable target device, without any user interaction, when the target device's Bluetooth is on, and it is running an app that offers a connectable BLE advertisement. An example of such an app could be a Bluetooth-based contact tracing app, such as Australia's COVIDSafe app, Singapore's TraceTogether app, or France's TousAntiCovid (formerly StopCovid). As part of the pairing process, two pieces (among others) of personally identifiable information are exchanged: the Identity Address of the Bluetooth adapter of the target device, and its associated Identity Resolving Key (IRK). Either one of these identifiers can be used to perform re-identification of the target device for long term tracking. The list of affected devices includes (but is not limited to): Galaxy Note 5, Galaxy S6 Edge, Galaxy A3, Tab A (2017), J2 Pro (2018), Galaxy Note 4, and Galaxy	N/A	H-SAM-GALA-040121/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S5. **CVE ID : CVE-2020-35693**		
Tendacn					
ac1200					
N/A	28-Dec-20	6.5	On Tenda AC1200 (Model AC6) 15.03.06.51_multi devices, admin, support, user, and nobody have a password of 1234. **CVE ID : CVE-2020-28093**	N/A	H-TEN-AC12-040121/1425
N/A	28-Dec-20	5	On Tenda AC1200 (Model AC6) 15.03.06.51_multi devices, the default settings for the router speed test contain links to download malware named elive or CNKI E-Learning. **CVE ID : CVE-2020-28094**	N/A	H-TEN-AC12-040121/1426
Tp-link					
archer_c5					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N,	N/A	H-TP--ARCH-040121/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wa901nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WA90-040121/1428
archer_c7					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND	N/A	H-TP--ARCH-040121/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
mr3420					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300	N/A	H-TP--MR34-040121/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. **CVE ID : CVE-2020-35575**		
mr6400					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--MR64-040121/1431
wa701nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400,	N/A	H-TP--WA70-040121/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wa801nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WA80-040121/1433
wdr3500					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WDR3-040121/1434
wdr3600					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N,	N/A	H-TP--WDR3-040121/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
we843n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WE84-040121/1436
wr1043nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to	N/A	H-TP--WR10-040121/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr1045nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND,	N/A	H-TP--WR10-040121/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr740n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WR74-040121/1439
wr741nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before	N/A	H-TP--WR74-040121/1440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr749n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices.	N/A	H-TP--WR74-040121/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-35575		
wr802n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WR80-040121/1442
wr840n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND,	N/A	H-TP--WR84-040121/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr841hp					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WR84-040121/1444
wr841n					
Insufficiently	26-Dec-20	7.5	A password-disclosure	N/A	H-TP--WR84-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		040121/1445
wr842n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N,	N/A	H-TP--WR84-040121/1446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr842nd					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WR84-040121/1447
wr845n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative	N/A	H-TP--WR84-040121/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr940n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N,	N/A	H-TP--WR94-040121/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr941hp					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WR94-040121/1450
wr945n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and	N/A	H-TP--WR94-040121/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**		
wr949n					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WR94-040121/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wrd4300					
Insufficiently Protected Credentials	26-Dec-20	7.5	A password-disclosure issue in the web interface on certain TP-Link devices allows a remote attacker to get full administrative access to the web panel. This affects WA901ND devices before 3.16.9(201211) beta, and Archer C5, Archer C7, MR3420, MR6400, WA701ND, WA801ND, WDR3500, WDR3600, WE843N, WR1043ND, WR1045ND, WR740N, WR741ND, WR749N, WR802N, WR840N, WR841HP, WR841N, WR842N, WR842ND, WR845N, WR940N, WR941HP, WR945N, WR949N, and WRD4300 devices. **CVE ID : CVE-2020-35575**	N/A	H-TP--WRD4-040121/1453
Wago					
750-8101\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
750-8102\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1455
750-8202\/000-012					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
750-8202\/000-022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1457
750-8202\/040-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
750-8202\/040-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1459
750-8206\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx)	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
750-8206\/025-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1461
750-8206\/040-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<=FW10. **CVE ID : CVE-2020-12522**		
750-8206\/040-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1463
750-8207\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10.	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12522		
750-8207\/025-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1465
750-8208\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
750-8208\/025-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1467
750-8210\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1468
750-8210\/040-000					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1469
750-8211\/040-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1470
750-8211\/040-001					
Improper	17-Dec-20	10	The reported vulnerability	https://cer	H-WAG-750--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	t.vde.com/en-us/advisories/vde-2020-045	040121/1471
750-8212\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1472
750-8212\/025-001					
Improper Neutralization	17-Dec-20	10	The reported vulnerability allows an attacker who has	https://cert.vde.com/e	H-WAG-750--040121/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Special Elements used in an OS Command ('OS Command Injection')			network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	n-us/advisories/vde-2020-045	
750-8212\/025-002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1474
750-8212\/040-000					
Improper Neutralization of Special	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the	https://cert.vde.com/en-	H-WAG-750--040121/1475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	us/advisories/vde-2020-045	
750-8212\/040-010					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1476
750-8213\/040-010					
Improper Neutralization of Special Elements used	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with	https://cert.vde.com/en-us/advisori	H-WAG-750--040121/1477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in an OS Command ('OS Command Injection')			specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	es/vde-2020-045	
750-8216\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1478
750-8216\/025-001					
Improper Neutralization of Special Elements used in an OS	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in	https://cert.vde.com/en-us/advisories/vde-	H-WAG-750--040121/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	2020-045	
750-8217\/025-000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-750--040121/1480
762-4301\/8000-002					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			(750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
762-4302\/8000-002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1482
762-4303\/8000-002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
762-4304\/8000-002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1484
762-5303\/8000-002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
762-5304\/8000-002					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1486
762-6201\/8000-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
762-6202\/8000-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1488
762-6203\/8000-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**		
762-6204\/8000-001					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-20	10	The reported vulnerability allows an attacker who has network access to the device to execute code with specially crafted packets in WAGO Series PFC 100 (750-81xx/xxx-xxx), Series PFC 200 (750-82xx/xxx-xxx), Series Wago Touch Panel 600 Standard Line (762-4xxx), Series Wago Touch Panel 600 Advanced Line (762-5xxx), Series Wago Touch Panel 600 Marine Line (762-6xxx) with firmware versions <=FW10. **CVE ID : CVE-2020-12522**	https://cert.vde.com/en-us/advisories/vde-2020-045	H-WAG-762--040121/1490
ZTE					
zxhn_e8810					
Origin Validation Error	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT	N/A	H-ZTE-ZXHN-040121/1491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6881**		
Insufficiently Protected Credentials	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6882**	N/A	H-ZTE-ZXHN-040121/1492
zxhn_e8820					
Origin Validation Error	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of abnormal messages. A remote attacker could	N/A	H-ZTE-ZXHN-040121/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6881**		
Insufficiently Protected Credentials	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6882**	N/A	H-ZTE-ZXHN-040121/1494
zxhn_e8822					
Origin Validation Error	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an MQTT DoS vulnerability, which is caused by the failure of the device to verify the validity of	N/A	H-ZTE-ZXHN-040121/1495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abnormal messages. A remote attacker could connect to the MQTT server and send an MQTT exception message to the specified device, which will cause the device to deny service. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6881**		
Insufficiently Protected Credentials	21-Dec-20	5	ZTE E8810/E8820/E8822 series routers have an information leak vulnerability, which is caused by hard-coded MQTT service access credentials on the device. The remote attacker could use this credential to connect to the MQTT server, so as to obtain information about other devices by sending specific topics. This affects:<ZXHN E8810, ZXHN E8820, ZXHN E8822><E8810 V1.0.26, E8810 V2.0.1, E8820 V1.1.3L, E8820 V2.0.13, E8822 V2.0.13> **CVE ID : CVE-2020-6882**	N/A	H-ZTE-ZXHN-040121/1496
Zyxel					
usg20-vpn					
Cleartext Storage of Sensitive	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account	http://ftp.zyxel.com/USG40/firm	H-ZYX-USG2-040121/1497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			(zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	ware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	
usg20w-vpn					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG2-040121/1498
usg40					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges.	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.sht	H-ZYX-USG4-040121/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29583	ml	
usg40w					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG4-040121/1500
usg60					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG6-040121/1501
usg60w					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf,	H-ZYX-USG6-040121/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	https://www.zyxel.com/support/CVE-2020-29583.shtml	
usg110					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG1-040121/1503
usg210					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG2-040121/1504
usg310					
Cleartext	22-Dec-20	2.1	Firmware version 4.60 of	http://ftp.z	H-ZYX-USG3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	yxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	040121/1505
usg1100					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG1-040121/1506
usg1900					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-	H-ZYX-USG1-040121/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with admin privileges. **CVE ID : CVE-2020-29583**	2020-29583.shtml	
usg2200					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-USG2-040121/1508
zywall110					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AALA.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-ZYWA-040121/1509
zywall310					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password.	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL	H-ZYX-ZYWA-040121/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	
zywall1100					
Cleartext Storage of Sensitive Information	22-Dec-20	2.1	Firmware version 4.60 of Zyxel USG devices contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges. **CVE ID : CVE-2020-29583**	http://ftp.zyxel.com/USG40/firmware/USG40_4.60(AAL A.1)C0_2.pdf, https://www.zyxel.com/support/CVE-2020-29583.shtml	H-ZYX-ZYWA-040121/1511