SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 05 January 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-20151	Trendnet AC2600 TEW-827DRU version 2.08B01 contains a flaw in the session management for the device. The router's management software manages web sessions based on IP address rather than verifying client cookies/session tokens/etc. This allows an attacker (whether from a different computer, different web browser on the same machine, etc.) to take over an existing session. This does require the attacker to be able to spoof or take over original IP address of the original user's session.	10.0	More Details
CVE-2022-21643	USOC is an open source CMS with a focus on simplicity. In affected versions USOC allows for SQL injection via register.php. In particular usernames, email addresses, and passwords provided by the user were not sanitized and were used directly to construct a sql statement. Users are advised to upgrade as soon as possible. There are not workarounds for this issue.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43832	Spinnaker is an open source, multi-cloud continuous delivery platform. Spinnaker has improper permissions allowing pipeline creation & execution. This lets an arbitrary user with access to the gate endpoint to create a pipeline and execute it without authentication. If users haven't setup Role-based access control (RBAC) with-in spinnaker, this enables remote execution and access to deploy almost any resources on any account. Patches are available on the latest releases of the supported branches and users are advised to upgrade as soon as possible. Users unable to upgrade should enable RBAC on ALL accounts and applications. This mitigates the ability of a pipeline to affect any accounts. Block application access unless permission are enabled. Users should make sure ALL application creation is restricted via appropriate wildcards.	10.0	More Details
CVE-2021-45427	Emerson XWEB 300D EVO 3.0.7--3ee403 is affected by: unauthenticated arbitrary file deletion due to path traversal. An attacker can browse and delete files without any authentication due to incorrect access control and directory traversal.	9.8	More Details
CVE-2021-20149	Trendnet AC2600 TEW-827DRU version 2.08B01 does not have sufficient access controls for the WAN interface. The default iptables ruleset for governing access to services on the device only apply to IPv4. All services running on the devices are accessible via the WAN interface via IPv6 by default.	9.8	More Details
CVE-2021-24042	The calling logic for WhatsApp for Android prior to v2.21.23, WhatsApp Business for Android prior to v2.21.23, WhatsApp for iOS prior to v2.21.230, WhatsApp Business for iOS prior to v2.21.230, WhatsApp for KaiOS prior to v2.2143, WhatsApp Desktop prior to v2.2146 could have allowed an out-of-bounds write if a user makes a 1:1 call to a malicious actor.	9.8	More Details
CVE-2022-0086	uppy is vulnerable to Server-Side Request Forgery (SSRF)	9.8	More Details
CVE-2021-45389	A flaw was found with the JWT token. A self-signed JWT token could be injected into the update manager and bypass the authentication process, thus could escalate privileges. This affects StarWind SAN and NAS build 1578 and StarWind Command Center build 6864.	9.8	More Details
CVE-2021-43711	The downloadFlile.cgi binary file in TOTOLINK EX200 V4.0.3c.7646_B20201211 has a command injection vulnerability when receiving GET parameters. The parameter name can be constructed for unauthenticated command execution.	9.8	More Details
CVE-2021-39990	The screen lock module has a Stack-based Buffer Overflow vulnerability.Successful exploitation of this vulnerability may affect user experience.	9.8	More Details
CVE-2021-39979	HHEE system has a Code Injection vulnerability.Successful exploitation of this vulnerability may affect HHEE system integrity.	9.8	More Details
CVE-2021-37128	HwPCAssistant has a Path Traversal vulnerability .Successful exploitation of this vulnerability may write any file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37121	There is a Configuration defects in Smartphone.Successful exploitation of this vulnerability may elevate the MEID (IMEI) permission.	9.8	More Details
CVE-2021-37120	There is a Double free vulnerability in Smartphone.Successful exploitation of this vulnerability may cause a kernel crash or privilege escalation.	9.8	More Details
CVE-2021-45428	TLR-2005KSH is affected by an incorrect access control vulnerability. THe PUT method is enabled so an attacker can upload arbitrary files including HTML and CGI formats.	9.8	More Details
CVE-2021-30351	An out of bound memory access can occur due to improper validation of number of frames being passed during music playback in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2021-45955	Dnsmasq 2.86 has a heap-based buffer overflow in resize_packet (called from FuzzResizePacket and fuzz_rfc1035.c) because of the lack of a proper bounds check upon pseudo header re-insertion. NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge." However, a contributor states that a security patch (mentioned in 016162.html) is needed	9.8	More Details
CVE-2021-45953	Dnsmasq 2.86 has a heap-based buffer overflow in extract_name (called from hash_questions and fuzz_util.c). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.	9.8	More Details
CVE-2021-20155	Trendnet AC2600 TEW-827DRU version 2.08B01 makes use of hardcoded credentials. It is possible to backup and restore device configurations via the management web interface. These devices are encrypted using a hardcoded password of "12345678".	9.8	More Details
CVE-2021-25981	In Talkyard, regular versions v0.2021.20 through v0.2021.33 and dev versions v0.2021.20 through v0.2021.34, are vulnerable to Insufficient Session Expiration. This may allow an attacker to reuse the admin’s still-valid session token even when logged-out, to gain admin privileges, given the attacker is able to obtain that token (via other, hypothetical attacks)	9.8	More Details
CVE-2022-0080	mruby is vulnerable to Heap-based Buffer Overflow	9.8	More Details
CVE-2021-45957	Dnsmasq 2.86 has a heap-based buffer overflow in answer_request (called from FuzzAnswerTheRequest and fuzz_rfc1035.c). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45956	Dnsmasq 2.86 has a heap-based buffer overflow in print_mac (called from log_packet and dhcp_reply). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.	9.8	More Details
CVE-2021-20158	Trendnet AC2600 TEW-827DRU version 2.08B01 contains an authentication bypass vulnerability. It is possible for an unauthenticated, malicous actor to force the change of the admin password due to a hidden administrative command.	9.8	More Details
CVE-2021-45951	Dnsmasq 2.86 has a heap-based buffer overflow in check_bad_address (called from check_for_bogus_wildcard and FuzzCheckForBogusWildcard). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.	9.8	More Details
CVE-2021-45952	Dnsmasq 2.86 has a heap-based buffer overflow in dhcp_reply (called from dhcp_packet and FuzzDhcp). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.	9.8	More Details
CVE-2021-45954	Dnsmasq 2.86 has a heap-based buffer overflow in extract_name (called from answer_auth and FuzzAuth). NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge.	9.8	More Details
CVE-2021-30276	Improper access control while doing XPU re-configuration dynamically can lead to unauthorized access to a secure resource in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking	9.3	More Details
CVE-2021-30275	Possible integer overflow in page alignment interface due to lack of address and size validation before alignment in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.3	More Details
CVE-2021-40525	Apache James ManagedSieve implementation alongside with the file storage for sieve scripts is vulnerable to path traversal, allowing reading and writing any file. This vulnerability had been patched in Apache James 3.6.1 and higher. We recommend the upgrade. Distributed and Cassandra based products are also not impacted.	9.1	More Details
CVE-2021-39982	Phone Manager application has a Improper Privilege Management vulnerability.Successful exploitation of this vulnerability may read and write arbitrary files by tampering with Phone Manager notifications.	9.1	More Details
CVE-2021-37116	PCManager has a Weaknesses Introduced During Design vulnerability .Successful exploitation of this vulnerability may cause that the PIN of the subscriber is changed.	9.1	More Details
CVE-2022-21644	USOC is an open source CMS with a focus on simplicity. In affected versions USOC allows for SQL injection via usersearch.php. In search terms provided by the user were not sanitized and were used directly to construct a sql statement. The only users permitted to search are site admins. Users are advised to upgrade as soon as possible. There are not workarounds for this issue.	9.1	More Details

CVE Number	Description	Base Score	Reference

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-20166	Netgear RAX43 version 1.0.3.96 contains a buffer overrun vulnerability. The URL parsing functionality in the cgi-bin endpoint of the router containers a buffer overrun issue that can redirection control flow of the applicaiton.	8.8	More Details
CVE-2021-43876	Microsoft SharePoint Elevation of Privilege Vulnerability	8.8	More Details
CVE-2021-20165	Trendnet AC2600 TEW-827DRU version 2.08B01 does not properly implement csrf protections. Most pages lack proper usage of CSRF protections or mitigations. Additionally, pages that do make use of CSRF tokens are trivially bypassable as the server does not appear to validate them properly (i.e. re-using an old token or finding the token thru some other method is possible).	8.8	More Details
CVE-2021-25994	In Userfrosting, versions v0.3.1 to v4.6.2 are vulnerable to Host Header Injection. By luring a victim application user to click on a link, an unauthenticated attacker can use the “forgot password” functionality to reset the victim’s password and successfully take over their account.	8.8	More Details
CVE-2021-25030	The Events Made Easy WordPress plugin before 2.2.36 does not sanitise and escape the search_text parameter before using it in a SQL statement via the eme_searchmail AJAX action, available to any authenticated users. As a result, users with a role as low as subscriber can call it and perform SQL injection attacks	8.8	More Details
CVE-2021-45379	Glewlwyd 2.0.0, fixed in 2.6.1 is affected by an incorrect access control vulnerability. One user can attempt to log in as another user without its password.	8.8	More Details
CVE-2021-20132	Quagga Services on D-Link DIR-2640 less than or equal to version 1.11B02 use default hard-coded credentials, which can allow a remote attacker to gain administrative access to the zebra or ripd those services. Both are running with root privileges on the router (i.e., as the "admin" user, UID 0).	8.8	More Details
CVE-2021-45960	In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45732	Netgear Nighthawk R6700 version 1.0.4.120 makes use of a hardcoded credential. It does not appear that normal users are intended to be able to manipulate configuration backups due to the fact that they are encrypted/obfuscated. By extracting the configuration using readily available public tools, a user can reconfigure settings not intended to be manipulated, repackage the configuration, and restore a backup causing these settings to be changed.	8.8	More Details
CVE-2021-20173	Netgear Nighthawk R6700 version 1.0.4.120 contains a command injection vulnerability in update functionality of the device. By triggering a system update check via the SOAP interface, the device is susceptible to command injection via preconfigured values.	8.8	More Details
CVE-2021-20159	Trendnet AC2600 TEW-827DRU version 2.08B01 is vulnerable to command injection. The system log functionality of the firmware allows for command injection as root by supplying a malformed parameter.	8.8	More Details
CVE-2021-43852	OroPlatform is a PHP Business Application Platform. In affected versions by sending a specially crafted request, an attacker could inject properties into existing JavaScript language construct prototypes, such as objects. Later this injection may lead to JS code execution by libraries that are vulnerable to Prototype Pollution. This issue has been patched in version 4.2.8. Users unable to upgrade may configure a firewall to drop requests containing next strings: `__proto__` , `constructor[prototype]`, and `constructor.prototype` to mitigate this issue.	8.8	More Details
CVE-2021-20160	Trendnet AC2600 TEW-827DRU version 2.08B01 contains a command injection vulnerability in the smb functionality of the device. The username parameter used when configuring smb functionality for the device is vulnerable to command injection as root.	8.8	More Details
CVE-2021-20170	Netgear RAX43 version 1.0.3.96 makes use of hardcoded credentials. It does not appear that normal users are intended to be able to manipulate configuration backups due to the fact that they are encrypted. This encryption is accomplished via a password-protected zip file with a hardcoded password (RAX50w!a4udk). By unzipping the configuration using this password, a user can reconfigure settings not intended to be manipulated, re-zip the configuration, and restore a backup causing these settings to be changed.	8.8	More Details
CVE-2021-44161	Changing MOTP (Mobile One Time Password) system’s specific function parameter has insufficient validation for user input. A attacker in local area network can perform SQL injection attack to read, modify or delete backend database without authentication.	8.8	More Details
CVE-2021-20134	Quagga Services on D-Link DIR-2640 less than or equal to version 1.11B02 are affected by an absolute path traversal vulnerability that allows a remote, authenticated attacker to set an arbitrary file on the router's filesystem as the log file used by either Quagga service (zebra or ripd). Subsequent log messages will be appended to the file, prefixed by a timestamp and some logging metadata. Remote code execution can be achieved by using this vulnerability to append to a shell script on the router's filesystem, and then awaiting or triggering the execution of that script. A remote, unauthenticated root shell can easily be obtained on the device in this fashion.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30262	Improper validation of a socket state when socket events are being sent to clients can lead to invalid access of memory in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-30274	Possible integer overflow in access control initialization interface due to lack and size and address validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-30282	Possible out of bound write in RAM partition table due to improper validation on number of partitions provided in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-30335	Possible assertion in QOS request due to improper validation when multiple add or update request are received simultaneously in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2021-30336	Possible out of bound read due to lack of domain input validation while processing APK close session request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearables	8.4	More Details
CVE-2021-30337	Possible use after free when process shell memory is freed using IOCTL call and process initialization is in progress in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.4	More Details
CVE-2022-21648	Latte is an open source template engine for PHP. Versions since 2.8.0 Latte has included a template sandbox and in affected versions it has been found that a sandbox escape exists allowing for injection into web pages generated from Latte. This may lead to XSS attacks. The issue is fixed in the versions 2.8.8, 2.9.6 and 2.10.8. Users unable to upgrade should not accept template input from untrusted sources.	8.2	More Details
CVE-2021-37134	Location-related APIs exists a Race Condition vulnerability.Successful exploitation of this vulnerability may use Higher Permissions for invoking the interface of location-related components.	8.1	More Details
CVE-2021-38687	A stack buffer overflow vulnerability has been reported to affect QNAP NAS running Surveillance Station. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of Surveillance Station: QTS 5.0.0 (64 bit): Surveillance Station 5.2.0.4.2 (2021/10/26) and later QTS 5.0.0 (32 bit): Surveillance Station 5.2.0.3.2 (2021/10/26) and later QTS 4.3.6 (64 bit): Surveillance Station 5.1.5.4.6 (2021/10/26) and later QTS 4.3.6 (32 bit): Surveillance Station 5.1.5.3.6 (2021/10/26) and later QTS 4.3.3: Surveillance Station 5.1.5.3.6 (2021/10/26) and later	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20167	Netgear RAX43 version 1.0.3.96 contains a command injection vulnerability. The readycloud cgi application is vulnerable to command injection in the name parameter.	8.0	More Details
CVE-2021-44158	ASUS RT-AX56U Wi-Fi Router is vulnerable to stack-based buffer overflow due to improper validation for httpd parameter length. An authenticated local area network attacker can launch arbitrary code execution to control the system or disrupt service.	8.0	More Details
CVE-2021-45917	The server-request receiver function of Shockwall system has an improper authentication vulnerability. An authenticated attacker of an agent computer within the local area network can use the local registry information to launch server-side request forgery (SSRF) attack on another agent computer, resulting in arbitrary code execution for controlling the system or disrupting service.	8.0	More Details
CVE-2021-30289	Possible buffer overflow due to lack of range check while processing a DIAG command for COEX management in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2021-4192	vim is vulnerable to Use After Free	7.8	More Details
CVE-2021-22045	VMware ESXi (7.0, 6.7 before ESXi670-202111101-SG and 6.5 before ESXi650-202110101-SG), VMware Workstation (16.2.0) and VMware Fusion (12.2.0) contains a heap-overflow vulnerability in CD-ROM device emulation. A malicious actor with access to a virtual machine with CD-ROM device emulation may be able to exploit this vulnerability in conjunction with other issues to execute code on the hypervisor from a virtual machine.	7.8	More Details
CVE-2021-20172	All known versions of the Netgear Genie Installer for macOS contain a local privilege escalation vulnerability. The installer of the macOS version of Netgear Genie handles certain files in an insecure way. A malicious actor who has local access to the endpoint on which the software is going to be installed may overwrite certain files to obtain privilege escalation to root.	7.8	More Details
CVE-2022-20012	In mdp driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05836478; Issue ID: ALPS05836478.	7.8	More Details
CVE-2021-45912	An unauthenticated Named Pipe channel in Controlup Real-Time Agent (cuAgent.exe) before 8.5 potentially allows an attacker to run OS commands via the ProcessActionRequest WCF method.	7.8	More Details
CVE-2021-45980	Foxit PDF Reader and PDF Editor before 11.1 on macOS allow remote attackers to execute arbitrary code via getURL in the JavaScript API.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45979	Foxit PDF Reader and PDF Editor before 11.1 on macOS allow remote attackers to execute arbitrary code via app.launchURL in the JavaScript API.	7.8	More Details
CVE-2021-45926	MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd0c689be0) in mdb_numeric_to_string (called from mdb_xfer_bound_data and _mdb_attempt_bind).	7.8	More Details
CVE-2021-45927	MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd6e029ee0) in mdb_numeric_to_string (called from mdb_xfer_bound_data and _mdb_attempt_bind).	7.8	More Details
CVE-2021-44852	An issue was discovered in BS_RCIO64.sys in Biostar RACING GT Evo 2.1.1905.1700. A low-integrity process can open the driver's device object and issue IOCTLs to read or write to arbitrary physical memory locations (or call an arbitrary address), leading to execution of arbitrary code. This is associated with 0x226040, 0x226044, and 0x226000.	7.8	More Details
CVE-2021-30303	Possible buffer overflow due to lack of buffer length check when segmented WMI command is received in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-45978	Foxit PDF Reader and PDF Editor before 11.1 on macOS allow remote attackers to execute arbitrary code via xfa.host.gotoURL in the XFA API.	7.8	More Details
CVE-2021-30267	Possible integer overflow to buffer overflow due to improper input validation in FTM ARA commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2021-30268	Possible heap Memory Corruption Issue due to lack of input validation when sending HWTC IQ Capture command in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2021-30279	Possible access control violation while setting current permission for VMIDs due to improper permission masking in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-41388	Netskope client prior to 89.x on macOS is impacted by a local privilege escalation vulnerability. The XPC implementation of nsAuxiliarySvc process does not perform validation on new connections before accepting the connection. Thus any low privileged user can connect and call external methods defined in XPC service as root, elevating their privilege to the highest level.	7.8	More Details
CVE-2021-4187	vim is vulnerable to Use After Free	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21647	CodeIgniter is an open source PHP full-stack web framework. Deserialization of Untrusted Data was found in the `old()` function in CodeIgniter4. Remote attackers may inject auto-loadable arbitrary objects with this vulnerability, and possibly execute existing PHP code on the server. We are aware of a working exploit, which can lead to SQL injection. Users are advised to upgrade to v4.1.6 or later. Users unable to upgrade as advised to not use the `old()` function and form_helper nor `RedirectResponse::withInput()` and `redirect()->withInput()`.	7.7	More Details
CVE-2022-21650	Convos is an open source multi-user chat that runs in a web browser. You can't use SVG extension in Convos' chat window, but you can upload a file with an .html extension. By uploading an SVG file with an html extension the upload filter can be bypassed. This causes Stored XSS. Also, after uploading a file the XSS attack is triggered upon a user viewing the file. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible.	7.6	More Details
CVE-2022-21649	Convos is an open source multi-user chat that runs in a web browser. Characters starting with "https://" in the chat window create an <a> tag. Stored XSS vulnerability using onfocus and autofocus occurs because escaping exists for "<" or ">" but escaping for double quotes does not exist. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible.	7.6	More Details
CVE-2020-23026	A NULL pointer dereference in the main() function dhry_1.c of dhrystone 2.1 causes a denial of service (DoS).	7.5	More Details
CVE-2021-39971	Password vault has a External Control of System or Configuration Setting vulnerability.Successful exploitation of this vulnerability could compromise confidentiality.	7.5	More Details
CVE-2021-39972	MyHuawei-App has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability.Successful exploitation of this vulnerability could compromise confidentiality.	7.5	More Details
CVE-2021-39973	There is a Null pointer dereference in Smartphones.Successful exploitation of this vulnerability may cause the kernel to break down.	7.5	More Details
CVE-2021-23727	This affects the package celery before 5.2.2. It by default trusts the messages and metadata stored in backends (result stores). When reading task metadata from the backend, the data is deserialized. Given that an attacker can gain access to, or somehow manipulate the metadata within a celery backend, they could trigger a stored command injection vulnerability and potentially gain further access to the system.	7.5	More Details
CVE-2021-39974	There is an Out-of-bounds read in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-40148	In Modem EMM, there is a possible information disclosure due to a missing data encryption. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00716585; Issue ID: ALPS05886933.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45885	An issue was discovered in Stormshield Network Security (SNS) 4.2.2 through 4.2.7 (fixed in 4.2.8). Under a specific update-migration scenario, the first SSH password change does not properly clear the old password.	7.5	More Details
CVE-2021-3842	nltk is vulnerable to Inefficient Regular Expression Complexity	7.5	More Details
CVE-2021-30293	Possible assertion due to lack of input validation in PUSCH configuration in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT	7.5	More Details
CVE-2021-39975	Hilinksvc has a Data Processing Errors vulnerability.Successful exploitation of this vulnerability may cause denial of service attacks.	7.5	More Details
CVE-2021-40110	In Apache James, using Jazzer fuzzer, we identified that an IMAP user can craft IMAP LIST commands to orchestrate a Denial Of Service using a vulnerable Regular expression. This affected Apache James prior to 3.6.1 We recommend upgrading to Apache James 3.6.1 or higher , which enforce the use of RE2J regular expression engine to execute regex in linear time without back-tracking.	7.5	More Details
CVE-2021-4188	mruby is vulnerable to NULL Pointer Dereference	7.5	More Details
CVE-2021-39983	The HwNearbyMain module has a Data Processing Errors vulnerability.Successful exploitation of this vulnerability may cause a process to restart.	7.5	More Details
CVE-2021-39977	The HwNearbyMain module has a NULL Pointer Dereference vulnerability.Successful exploitation of this vulnerability may cause a process to restart.	7.5	More Details
CVE-2021-34797	Apache Geode versions up to 1.12.4 and 1.13.4 are vulnerable to a log file redaction of sensitive information flaw when using values that begin with characters other than letters or numbers for passwords and security properties with the prefix "sysprop-", "javax.net.ssl", or "security-". This issue is fixed by overhauling the log file redaction in Apache Geode versions 1.12.5, 1.13.5, and 1.14.0.	7.5	More Details
CVE-2021-39978	Telephony application has a SQL Injection vulnerability.Successful exploitation of this vulnerability may cause privacy and security issues.	7.5	More Details
CVE-2021-41817	Date.parse in the date gem through 3.2.0 for Ruby allows ReDoS (regular expression Denial of Service) via a long string. The fixed versions are 3.2.1, 3.1.2, 3.0.2, and 2.0.1.	7.5	More Details
CVE-2021-44716	net/http in Go before 1.16.12 and 1.17.x before 1.17.5 allows uncontrolled memory consumption in the header canonicalization cache via HTTP/2 requests.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30273	Possible assertion due to improper handling of IPV6 packet with invalid length in destination options header in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	7.5	More Details
CVE-2021-41819	CGI::Cookie.parse in Ruby through 2.6.8 mishandles security prefixes in cookie names. This also affects the CGI gem through 0.3.0 for Ruby.	7.5	More Details
CVE-2021-39989	The HwNearbyMain module has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability.Successful exploitation of this vulnerability may cause a process to restart.	7.5	More Details
CVE-2021-39988	The HwNearbyMain module has a NULL Pointer Dereference vulnerability.Successful exploitation of this vulnerability may cause a process to restart.	7.5	More Details
CVE-2021-39987	The HwNearbyMain module has a Data Processing Errors vulnerability.Successful exploitation of this vulnerability may cause a process to restart.	7.5	More Details
CVE-2021-39985	The HwNearbyMain module has a Improper Validation of Array Index vulnerability.Successful exploitation of this vulnerability may cause a process to restart.	7.5	More Details
CVE-2021-39970	HwPCAssistant has a Improper Input Validation vulnerability.Successful exploitation of this vulnerability may create any file with the system app permission.	7.5	More Details
CVE-2021-39969	There is an Unauthorized file access vulnerability in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-24831	All AJAX actions of the Tab WordPress plugin before 1.3.2 are available to both unauthenticated and authenticated users, allowing unauthenticated attackers to modify various data in the plugin, such as add/edit/delete arbitrary tabs.	7.5	More Details
CVE-2021-4184	Infinite loop in the BitTorrent DHT dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-37098	Hilinksvc service exists a Data Processing Errors vulnerability .Successful exploitation of this vulnerability may cause application crash.	7.5	More Details
CVE-2021-37110	There is a Timing design defects in Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-37111	There is a Memory leakage vulnerability in Smartphone.Successful exploitation of this vulnerability may cause memory exhaustion.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20157	It is possible for an unauthenticated, malicious user to force the device to reboot due to a hidden administrative command.	7.5	More Details
CVE-2021-20174	Netgear Nighthawk R6700 version 1.0.4.120 does not utilize secure communication methods to the web interface. By default, all communication to/from the device's web interface is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext.	7.5	More Details
CVE-2021-20175	Netgear Nighthawk R6700 version 1.0.4.120 does not utilize secure communication methods to the SOAP interface. By default, all communication to/from the device's SOAP Interface (port 5000) is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext	7.5	More Details
CVE-2021-37113	There is a Privilege escalation vulnerability with the file system component in Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-37117	There is a Service logic vulnerability in Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS.	7.5	More Details
CVE-2021-45077	Netgear Nighthawk R6700 version 1.0.4.120 stores sensitive information in plaintext. All usernames and passwords for the device's associated services are stored in plaintext on the device. For example, the admin password is stored in plaintext in the primary configuration file on the device.	7.5	More Details
CVE-2021-37119	There is a Service logic vulnerability in Smartphone.Successful exploitation of this vulnerability may cause WLAN DoS.	7.5	More Details
CVE-2021-24893	The Stars Rating WordPress plugin before 3.5.1 does not validate the submitted rating, allowing submission of long integer, causing a Denial of Service in the comments section, or pending comment dashboard depending if the user sent it as unauthenticated or authenticated.	7.5	More Details
CVE-2021-4182	Crash in the RFC 7468 dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-4181	Crash in the Sysdig Event dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-4185	Infinite loop in the RTMPT dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-39966	There is an Uninitialized AOD driver structure in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39968	Changlian Blocklist has a Business Logic Errors vulnerability .Successful exploitation of this vulnerability may expand the attack surface of the message class.	7.5	More Details
CVE-2021-39967	There is a Vulnerability of obtaining broadcast information improperly due to improper broadcast permission settings in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-3845	ws-scrcpy is vulnerable to External Control of File Name or Path	7.5	More Details
CVE-2021-37125	Arbitrary file has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability .Successful exploitation of this vulnerability may cause confidentiality is affected.	7.5	More Details
CVE-2021-39984	Huawei idap module has a Out-of-bounds Read vulnerability.Successful exploitation of this vulnerability may cause Denial of Service.	7.5	More Details
CVE-2021-38576	A BIOS bug in firmware for a particular PC model leaves the Platform authorization value empty. This can be used to permanently brick the TPM in multiple ways, as well as to non-permanently DoS the system.	7.5	More Details
CVE-2021-37133	There is an Unauthorized file access vulnerability in Smartphones.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2021-37126	Arbitrary file has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability .Successful exploitation of this vulnerability may cause the directory is traversed.	7.5	More Details
CVE-2021-20154	Trendnet AC2600 TEW-827DRU version 2.08B01 contains an security flaw in the web interface. HTTPS is not enabled on the device by default. This results in cleartext transmission of sensitive information such as passwords.	7.5	More Details
CVE-2021-4190	Large loop in the Kafka dissector in Wireshark 3.6.0 allows denial of service via packet injection or crafted capture file	7.5	More Details
CVE-2021-35034	An insufficient session expiration vulnerability in the CGI program of the Zyxel NBG6604 firmware could allow a remote attacker to access the device if the correct token can be intercepted.	7.4	More Details
CVE-2021-30271	Possible null pointer dereference in trap handler due to lack of thread ID validation before dereferencing it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30270	Possible null pointer dereference in thread profile trap handler due to lack of thread ID validation before dereferencing it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.3	More Details
CVE-2021-30269	Possible null pointer dereference due to lack of TLB validation for user provided address in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.3	More Details
CVE-2021-30272	Possible null pointer dereference in thread cache operation handler due to lack of validation of user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.3	More Details
CVE-2021-44160	Carinal Tien Hospital Health Report System's login page has improper authentication, a remote attacker can acquire another general user's privilege by modifying the cookie parameter without authentication. The attacker can then perform limited operations on the system or modify data, making the service partially unavailable to the user.	7.3	More Details
CVE-2021-44466	Bitmask Riseup VPN 0.21.6 contains a local privilege escalation flaw due to improper access controls. When the software is installed with a non-default installation directory off of the system root, the installer fails to properly set ACLs. This allows lower privileged users to replace the VPN executable with a malicious one. When a higher privileged user such as an Administrator launches that executable, it is possible for the lower privileged user to escalate to Administrator privileges.	7.3	More Details
CVE-2020-11263	An integer overflow due to improper check performed after the address and size passed are aligned in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	7.3	More Details
CVE-2021-25023	The Speed Booster Pack PageSpeed Optimization Suite WordPress plugin before 4.3.3.1 does not escape the sbp_convert_table_name parameter before using it in a SQL statement to convert the related table, leading to an SQL injection	7.2	More Details
CVE-2021-43861	Mermaid is a Javascript based diagramming and charting tool that uses Markdown-inspired text definitions and a renderer to create and modify complex diagrams. Prior to version 8.13.8, malicious diagrams can run javascript code at diagram readers' machines. Users should upgrade to version 8.13.8 to receive a patch. There are no known workarounds aside from upgrading.	7.2	More Details
CVE-2021-24786	The Download Monitor WordPress plugin before 4.4.5 does not properly validate and escape the "orderby" GET parameter before using it in a SQL statement when viewing the logs, leading to an SQL Injection issue	7.2	More Details
CVE-2021-45913	A hardcoded key in ControlUp Real-Time Agent (cuAgent.exe) before 8.2.5 may allow a potential attacker to run OS commands via a WCF channel.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30278	Improper input validation in TrustZone memory transfer interface can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.1	More Details
CVE-2021-36722	Emuse - eServices / eNvoice SQL injection can be used in various ways ranging from bypassing login authentication or dumping the whole database to full RCE on the affected endpoints. The SQLi caused by CWE-209: Generation of Error Message Containig Sensetive Information, showing parts of the aspx code and the webroot location , information an attacker can leverage to further compromise the host.	7.1	More Details
CVE-2021-38688	An improper authentication vulnerability has been reported to affect Android App Qfile. If exploited, this vulnerability allows attackers to compromise app and access information We have already fixed this vulnerability in the following versions of Qfile: Qfile 3.0.0.1105 and later	7.1	More Details
CVE-2021-31833	Potential product security bypass vulnerability in McAfee Application and Change Control (MACC) prior to version 8.3.4 allows a locally logged in attacker to circumvent the application solidification protection provided by MACC, permitting them to run applications that would usually be prevented by MACC. This would require the attacker to rename the specified binary to match name of any configured updater and perform a specific set of steps, resulting in the renamed binary to be to run.	7.1	More Details
CVE-2021-30283	Possible denial of service due to improper handling of debug register trap from user applications in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.1	More Details
CVE-2021-1894	Improper access control in TrustZone due to improper error handling while handling the signing key in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.1	More Details
CVE-2021-45972	The giftrans function in giftrans 1.12.2 contains a stack-based buffer overflow because a value inside the input file determines the amount of data to write. This allows an attacker to overwrite up to 250 bytes outside of the allocated buffer with arbitrary data.	7.1	More Details
CVE-2021-41236	OroPlatform is a PHP Business Application Platform. In affected versions the email template preview is vulnerable to XSS payload added to email template content. An attacker must have permission to create or edit an email template. For successful payload, execution the attacked user must preview a vulnerable email template. There are no workarounds that address this vulnerability. Users are advised to upgrade as soon as is possible.	6.9	More Details
CVE-2021-20168	Netgear RAX43 version 1.0.3.96 does not have sufficient protections to the UART interface. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection, login with default credentials, and execute commands as the root user. These default credentials are admin:admin.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20153	Trendnet AC2600 TEW-827DRU version 2.08B01 contains a symlink vulnerability in the bittorrent functionality. If enabled, the bittorrent functionality is vulnerable to a symlink attack that could lead to remote code execution on the device. If an end user inserts a flash drive with a malicious symlink on it that the bittorrent client can write downloads to, then a user is able to download arbitrary files to any desired location on the devices filesystem, which could lead to remote code execution. Example directories vulnerable to this include "config", "downloads", and "torrents", though it should be noted that "downloads" is the only vector that allows for arbitrary files to be downloaded to arbitrary locations.	6.8	More Details
CVE-2021-20872	Protection mechanism failure vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, bizhub 4752/4052 GC9-X4 and earlier) allows a physical attacker to bypass the firmware integrity verification and to install malicious firmware.	6.8	More Details
CVE-2021-23147	Netgear Nighthawk R6700 version 1.0.4.120 does not have sufficient protections for the UART console. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection and execute commands as the root user without authentication.	6.8	More Details
CVE-2021-20169	Netgear RAX43 version 1.0.3.96 does not utilize secure communications to the web interface. By default, all communication to/from the device is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext.	6.8	More Details
CVE-2021-43850	Discourse is an open source platform for community discussion. In affected versions admins users can trigger a Denial of Service attack via the `/message-bus/_diagnostics` path. The impact of this vulnerability is greater on multisite Discourse instances (where multiple forums are served from a single application server) where any admin user on any of the forums are able to visit the `/message-bus/_diagnostics` path. The problem has been patched. Please upgrade to 2.8.0.beta10 or 2.7.12. No workarounds for this issue exist.	6.8	More Details
CVE-2021-20161	Trendnet AC2600 TEW-827DRU version 2.08B01 does not have sufficient protections for the UART functionality. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection. No username or password is required and the user is given a root shell with full control of the device.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20016	In vow driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862986; Issue ID: ALPS05862986.	6.7	More Details
CVE-2021-30298	Possible out of bound access due to improper validation of item size and DIAG memory pools data while switching between USB and PCIE interface in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2022-20014	In vow driver, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05857308; Issue ID: ALPS05857308.	6.7	More Details
CVE-2021-39143	Spinnaker is an open source, multi-cloud continuous delivery platform. A path traversal vulnerability was discovered in uses of TAR files by AppEngine for deployments. This uses a utility to extract files locally for deployment without validating the paths in that deployment don't override system files. This would allow an attacker to override files on the container, POTENTIALLY introducing a MITM type attack vector by replacing libraries or injecting wrapper files. Users are advised to update as soon as possible. For users unable to update disable Google AppEngine deployments and/or disable artifacts that provide TARs.	6.6	More Details
CVE-2022-20023	In Bluetooth, there is a possible application crash due to bluetooth flooding a device with LMP_AU_rand packet. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198608; Issue ID: ALPS06198608.	6.5	More Details
CVE-2021-45941	libbpf 0.6.0 and 0.6.1 has a heap-based buffer overflow (8 bytes) in __bpf_object__open (called from bpf_object__open_mem and bpf-object-fuzzer.c).	6.5	More Details
CVE-2022-20021	In Bluetooth, there is a possible application crash due to bluetooth does not properly handle the reception of multiple LMP_host_connection_req. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198513; Issue ID: ALPS06198513.	6.5	More Details
CVE-2021-20156	Trendnet AC2600 TEW-827DRU version 2.08B01 contains an improper access control configuration that could allow for a malicious firmware update. It is possible to manually install firmware that may be malicious in nature as there does not appear to be any signature validation done to determine if it is from a known and trusted source. This includes firmware updates that are done via the automated "check for updates" in the admin interface. If an attacker is able to masquerade as the update server, the device will not verify that the firmware updates downloaded are legitimate.	6.5	More Details
CVE-2020-29292	iBall WRD12EN 1.0.0 devices allow cross-site request forgery (CSRF) attacks as demonstrated by enabling DNS settings or modifying the range for IP addresses.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20022	In Bluetooth, there is a possible link disconnection due to bluetooth does not properly handle a connection attempt from a host with the same BD address as the currently connected BT host. This could lead to remote denial of service of bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198578; Issue ID: ALPS06198578.	6.5	More Details
CVE-2021-44674	An information exposure issue has been discovered in Opmantek Open-AudIT 4.2.0. The vulnerability allows an authenticated attacker to read file outside of the restricted directory.	6.5	More Details
CVE-2021-45950	LibreDWG 0.12.4.4313 through 0.12.4.4367 has an out-of-bounds write in dwg_free_BLOCK_private (called from dwg_free_BLOCK and dwg_free_object).	6.5	More Details
CVE-2021-45940	libbpf 0.6.0 and 0.6.1 has a heap-based buffer overflow (4 bytes) in __bpf_object__open (called from bpf_object__open_mem and bpf-object-fuzzer.c).	6.5	More Details
CVE-2021-20152	Trendnet AC2600 TEW-827DRU version 2.08B01 lacks proper authentication to the bittorrent functionality. If enabled, anyone is able to visit and modify settings and files via the Bittorent web client by visiting: http://192.168.10.1:9091/transmission/web/	6.5	More Details
CVE-2021-1918	Improper handling of resource allocation in virtual machines can lead to information exposure in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	6.5	More Details
CVE-2021-35093	Possible memory corruption in BT controller when it receives an oversized LMP packet over 2-DH1 link and leads to denial of service in BlueCore	6.5	More Details
CVE-2021-45931	HarfBuzz 2.9.0 has an out-of-bounds write in hb_bit_set_invertible_t::set (called from hb_sparseset_t<hb_bit_set_invertible_t>::set and hb_set_copy).	6.5	More Details
CVE-2021-41789	In wifi driver, there is a possible system crash due to a missing validation check. This could lead to remote denial of service from a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20190426015; Issue ID: GN20190426015.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20869	Exposure of sensitive information to an unauthorized actor vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, and bizhub 4752/4052 GC9-X4 and earlier) allows an attacker on the adjacent network to obtain some of user credentials if LDAP server authentication is enabled via a specific SOAP message.	6.5	More Details
CVE-2021-43333	The Datalogic DXU service on (for example) DL-Axist devices does not require authentication for configuration changes or disclosure of configuration settings.	6.5	More Details
CVE-2021-20871	Exposure of sensitive information to an unauthorized actor vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, and bizhub 4752/4052 GC9-X4 and earlier) allows an attacker on the adjacent network to obtain the credentials if the destination information including credentials are registered in the address book via a specific SOAP message.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40111	In Apache James, while fuzzing with Jazzer the IMAP parsing stack, we discover that crafted APPEND and STATUS IMAP command could be used to trigger infinite loops resulting in expensive CPU computations and OutOfMemory exceptions. This can be used for a Denial Of Service attack. The IMAP user needs to be authenticated to exploit this vulnerability. This affected Apache James prior to version 3.6.1. This vulnerability had been patched in Apache James 3.6.1 and higher. We recommend the upgrade.	6.5	More Details
CVE-2021-30348	Improper validation of LLM utility timers availability can lead to denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	6.5	More Details
CVE-2022-20013	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837742; Issue ID: ALPS05837742.	6.4	More Details
CVE-2021-4186	Crash in the Gryphon dissector in Wireshark 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2021-43677	Fluxbb v1.4.12 is affected by a Cross Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-46109	Invalid input sanitizing leads to reflected Cross Site Scripting (XSS) in ASUS RT-AC52U_B1 3.0.0.4.380.10931 can lead to a user session hijack.	6.1	More Details
CVE-2021-43942	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Reflected Cross-Site Scripting (XSS) vulnerability in the /rest/collectors/1.0/template/custom endpoint. To exploit this issue, the attacker must trick a user into visiting a malicious website. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.	6.1	More Details
CVE-2021-24999	The Booster for WooCommerce WordPress plugin before 5.4.9 does not sanitise and escape the wcj_notice parameter before outputting it back in the admin dashboard when the Pdf Invoicing module is enabled, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-25001	The Booster for WooCommerce WordPress plugin before 5.4.9 does not sanitise and escape the wcj_create_products_xml_result parameter before outputting back in the admin dashboard when the Product XML Feeds module is enabled, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-44896	DMP Roadmap before 3.0.4 allows XSS.	6.1	More Details
CVE-2021-4176	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45818	SAFARI Montage 8.7.32 is affected by a CRLF injection vulnerability which can lead to HTTP response splitting.	6.1	More Details
CVE-2021-38876	IBM i 7.2, 7.3, and 7.4 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: 208404.	6.1	More Details
CVE-2021-24964	The LiteSpeed Cache WordPress plugin before 4.4.4 does not properly verify that requests are coming from QUIC.cloud servers, allowing attackers to make requests to certain endpoints by using a specific X-Forwarded-For header value. In addition, one of the endpoint could be used to set CSS code if a setting is enabled, which will then be output in some pages without being sanitised and escaped. Combining those two issues, an unauthenticated attacker could put Cross-Site Scripting payloads in pages visited by users.	6.1	More Details
CVE-2021-24973	The Site Reviews WordPress plugin before 5.17.3 does not sanitise and escape the site-reviews parameter of the glsr_action AJAX action (available to unauthenticated and any authenticated users), allowing them to perform Cross-Site Scripting attacks against logged in admins viewing the Tool dashboard of the plugin	6.1	More Details
CVE-2021-25000	The Booster for WooCommerce WordPress plugin before 5.4.9 does not sanitise and escape the wcj_delete_role parameter before outputting back in the admin dashboard when the General module is enabled, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-36724	ForeScout - SecureConnector Local Service DoS - A low privilaged user which doesn't have permissions to shutdown the secure connector service writes a large amount of characters in the installationPath. This will cause the buffer to overflow and override the stack cookie causing the service to crash.	6.1	More Details
CVE-2021-25016	The Chaty WordPress plugin before 2.8.3 and Chaty Pro WordPress plugin before 2.8.2 do not sanitise and escape the search parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-45815	Quectel UC20 UMTS/HSPA+ UC20 6.3.14 is affected by a Cross Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2021-25027	The PowerPack Addons for Elementor WordPress plugin before 2.6.2 does not escape the tab parameter before outputting it back in an attribute in the admin dashboard, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-25040	The Booking Calendar WordPress plugin before 8.9.2 does not sanitise and escape the booking_type parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-25022	The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.16.66 does not sanitise and escape the backup_timestamp and job_id parameter before outputting then back in admin pages, leading to Reflected Cross-Site Scripting issues	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3837	openwhyd is vulnerable to Improper Authorization	6.1	More Details
CVE-2021-20133	Quagga Services on D-Link DIR-2640 less than or equal to version 1.11B02 are affected by an absolute path traversal vulnerability that allows a remote, authenticated attacker to set the "message of the day" banner to any file on the system, allowing them to read all or some of the contents of those files. Such sensitive information as hashed credentials, hardcoded plaintext passwords for other services, configuration files, and private keys can be disclosed in this fashion. Improper handling of filenames that identify virtual resources, such as "/dev/urandom" allows an attacker to effect a denial of service attack against the command line interfaces of the Quagga services (zebra and ripd).	6.1	More Details
CVE-2021-36723	Emuse - eServices / eNvoice Exposure Of Private Personal Information due to lack of identification mechanisms and predictable IDs an attacker can scrape all the files on the service.	6.1	More Details
CVE-2021-38542	Apache James prior to release 3.6.1 is vulnerable to a buffering attack relying on the use of the STARTTLS command. This can result in Man-in -the-middle command injection attacks, leading potentially to leakage of sensible information.	5.9	More Details
CVE-2021-41141	PJSIP is a free and open source multimedia communication library written in the C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In various parts of PJSIP, when error/failure occurs, it is found that the function returns without releasing the currently held locks. This could result in a system deadlock, which cause a denial of service for the users. No release has yet been made which contains the linked fix commit. All versions up to an including 2.11.1 are affected. Users may need to manually apply the patch.	5.9	More Details
CVE-2021-25991	In Ifme, versions v5.0.0 to v7.32 are vulnerable against an improper access control, which makes it possible for admins to ban themselves leading to their deactivation from Ifme account and complete loss of admin access to Ifme.	5.7	More Details
CVE-2021-45936	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttDecode_Disconnect (called from MqttClient_DecodePacket and MqttClient_WaitType).	5.5	More Details
CVE-2021-20171	Netgear RAX43 version 1.0.3.96 stores sensitive information in plaintext. All usernames and passwords for the device's associated services are stored in plaintext on the device. For example, the admin password is stored in plaintext in the primary configuration file on the device.	5.5	More Details
CVE-2021-45829	HDF5 1.13.1-1 is affected by: segmentation fault, which causes a Denial of Service.	5.5	More Details
CVE-2021-45937	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Connect).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45939	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Subscribe).	5.5	More Details
CVE-2021-45938	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Unsubscribe).	5.5	More Details
CVE-2021-4183	Crash in the pcapng file parser in Wireshark 3.6.0 allows denial of service via crafted capture file	5.5	More Details
CVE-2021-45946	Wasm3 0.5.0 has an out-of-bounds write in CompileBlock (called from Compile_LoopOrBlock and CompileBlockStatements).	5.5	More Details
CVE-2021-45932	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow (4 bytes) in MqttDecode_Publish (called from MqttClient_DecodePacket and MqttClient_HandlePacket).	5.5	More Details
CVE-2021-45935	Grok 9.5.0 has a heap-based buffer overflow in openhtj2k::T1OpenHTJ2K::decompress (called from std::__1::__packaged_task_func<std::__1::__bind<grk::T1DecompressScheduler::deco and std::__1::packaged_task<int).	5.5	More Details
CVE-2021-45958	UltraJSON (aka ujson) through 5.1.0 has a stack-based buffer overflow in Buffer_AppendIndentUnchecked (called from encode). Exploitation can, for example, use a large amount of indentation.	5.5	More Details
CVE-2021-45947	Wasm3 0.5.0 has an out-of-bounds write in Runtime_Release (called from EvaluateExpression and InitDataSegments).	5.5	More Details
CVE-2021-45948	Open Asset Import Library (aka assimp) 5.1.0 and 5.1.1 has a heap-based buffer overflow in _m3d_safestr (called from m3d_load and Assimp::M3DWrapper::M3DWrapper).	5.5	More Details
CVE-2021-45949	Ghostscript GhostPDL 9.50 through 9.54.0 has a heap-based buffer overflow in sampled_data_finish (called from sampled_data_continue and interp).	5.5	More Details
CVE-2022-20020	In libvcodecdrv, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05943906; Issue ID: ALPS05943906.	5.5	More Details
CVE-2022-20019	In libMtkOmxGsmDec, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05917620; Issue ID: ALPS05917620.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45944	Ghostscript GhostPDL 9.50 through 9.53.3 has a use-after-free in sampled_data_sample (called from sampled_data_continue and interp).	5.5	More Details
CVE-2021-45929	Wasm3 0.5.0 has an out-of-bounds write in CompileBlock (called from CompileElseBlock and Compile_If).	5.5	More Details
CVE-2021-45934	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_HandlePacket and MqttClient_WaitType).	5.5	More Details
CVE-2021-4193	vim is vulnerable to Out-of-bounds Read	5.5	More Details
CVE-2021-45928	libjxl b02d6b9, as used in libvips 8.11 through 8.11.2 and other products, has an out-of-bounds write in jxl::ModularFrameDecoder::DecodeGroup (called from jxl::FrameDecoder::ProcessACGroup and jxl::ThreadPool::RunCallState<jxl::FrameDecoder::ProcessSections).	5.5	More Details
CVE-2021-45930	Qt SVG in Qt 5.0.0 through 5.15.2 and 6.0.0 through 6.2.1 has an out-of-bounds write in QtPrivate::QCommonArrayOps<QPainterPath::Element>::growAppend (called from QPainterPath::addPath and QPathClipper::intersect).	5.5	More Details
CVE-2021-45942	OpenEXR 3.1.x before 3.1.4 has a heap-based buffer overflow in Imf_3_1::LineCompositeTask::execute (called from IlmThread_3_1::NullThreadPoolProvider::addTask and IlmThread_3_1::ThreadPool::addGlobalTask). NOTE: db217f2 may be inapplicable.	5.5	More Details
CVE-2021-45933	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow (8 bytes) in MqttDecode_Publish (called from MqttClient_DecodePacket and MqttClient_HandlePacket).	5.5	More Details
CVE-2021-45943	GDAL 3.3.0 through 3.4.0 has a heap-based buffer overflow in PCIDSK::CPCIDSKFile::ReadFromFile (called from PCIDSK::CPCIDSKSegment::ReadFromFile and PCIDSK::CPCIDSKBinarySegment::CPCIDSKBinarySegment).	5.5	More Details
CVE-2021-25990	In “ifme”, versions v7.22.0 to v7.31.4 are vulnerable against self-stored XSS in the contacts field as it allows loading XSS payloads fetched via an iframe.	5.4	More Details
CVE-2021-25989	In “ifme”, versions 1.0.0 to v7.31.4 are vulnerable against stored XSS vulnerability in the markdown editor. It can be exploited by making a victim a Leader of a group which triggers the payload for them.	5.4	More Details
CVE-2021-24828	The Mortgage Calculator / Loan Calculator WordPress plugin before 1.5.17 does not escape the some of the attributes of its mlcalc shortcode before outputting them, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4175	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2022-22293	admin/limits.php in Dolibarr 7.0.2 allows HTML injection, as demonstrated by the MAIN_MAX_DECIMALS_TOT parameter.	5.4	More Details
CVE-2021-25988	In “ifme”, versions 1.0.0 to v7.31.4 are vulnerable against stored XSS vulnerability (notifications section) which can be directly triggered by sending an ally request to the admin.	5.4	More Details
CVE-2021-25993	In Requarks wiki.js, versions 2.0.0-beta.147 to 2.5.255 are affected by Stored XSS vulnerability, where a low privileged (editor) user can upload a SVG file that contains malicious JavaScript while uploading assets in the page. That will send the JWT tokens to the attacker’s server and will lead to account takeover when accessed by the victim.	5.4	More Details
CVE-2021-24680	The WP Travel Engine WordPress plugin before 5.3.1 does not escape the Description field in the Trip Destination/Activities/Trip Type and Pricing Category pages, allowing users with a role as low as editor to perform Stored Cross-Site Scripting attacks, even when the unfiltered_html capability is disallowed	5.4	More Details
CVE-2021-20147	ManageEngine ADSelfService Plus below build 6116 contains an observable response discrepancy in the UMCP operation of the ChangePasswordAPI. This allows an unauthenticated remote attacker to determine whether a Windows domain user exists.	5.3	More Details
CVE-2021-37112	Hisuite module has a External Control of System or Configuration Setting vulnerability.Successful exploitation of this vulnerability may lead to Firmware leak.	5.3	More Details
CVE-2021-37114	There is an Out-of-bounds read vulnerability in Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	5.3	More Details
CVE-2021-37118	The HwNearbyMain module has a Improper Handling of Exceptional Conditions vulnerability.Successful exploitation of this vulnerability may lead to message leak.	5.3	More Details
CVE-2021-37132	PackageManagerService has a Permissions, Privileges, and Access Controls vulnerability .Successful exploitation of this vulnerability may cause that Third-party apps can obtain the complete list of Harmony apps without permission.	5.3	More Details
CVE-2022-0083	livehelperchat is vulnerable to Generation of Error Message Containing Sensitive Information	5.3	More Details
CVE-2021-38680	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Kazoo Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Kazoo Server: Kazoo Server 4.11.20 and later	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39980	Telephony application has a Exposure of Sensitive Information to an Unauthorized Actor vulnerability.Successful exploitation of this vulnerability could lead to sensitive information disclosure.	5.3	More Details
CVE-2021-39981	Chang Lian application has a vulnerability which can be maliciously exploited to hide the calling number.Successful exploitation of this vulnerability allows you to make an anonymous call.	5.3	More Details
CVE-2022-0079	showdoc is vulnerable to Generation of Error Message Containing Sensitive Information	5.3	More Details
CVE-2021-20150	Trendnet AC2600 TEW-827DRU version 2.08B01 improperly discloses information via redirection from the setup wizard. Authentication can be bypassed and a user may view information as Admin by manually browsing to the setup wizard and forcing it to redirect to the desired page.	5.3	More Details
CVE-2021-35035	A cleartext storage of sensitive information vulnerability in the Zyxel NBG6604 firmware could allow a remote, authenticated attacker to obtain sensitive information from the configuration file.	4.9	More Details
CVE-2021-20163	Trendnet AC2600 TEW-827DRU version 2.08B01 leaks information via the ftp web page. Usernames and passwords for all ftp users are revealed in plaintext on the ftpserver.asp page.	4.9	More Details
CVE-2021-25020	The CAOS	Host Google Analytics Locally WordPress plugin before 4.1.9 does not validate the cache directory setting, allowing high privilege users to use a path traversal vector and delete arbitrary folders when uninstalling the plugin	4.9	More Details
CVE-2021-20162	Trendnet AC2600 TEW-827DRU version 2.08B01 stores credentials in plaintext. Usernames and passwords are stored in plaintext in the config files on the device. For example, /etc/config/cameo contains the admin password in plaintext.	4.9	More Details
CVE-2021-25021	The OMGF	Host Google Fonts Locally WordPress plugin before 4.5.12 does not validate the cache directory setting, allowing high privilege users to use a path traversal vector and delete arbitrary folders when uninstalling the plugin	4.9	More Details
CVE-2021-20164	Trendnet AC2600 TEW-827DRU version 2.08B01 improperly discloses credentials for the smb functionality of the device. Usernames and passwords for all smb users are revealed in plaintext on the smbserver.asp page.	4.9	More Details
CVE-2021-44717	Go before 1.16.12 and 1.17.x before 1.17.5 on UNIX allows write operations to an unintended file or unintended network connection as a consequence of erroneous closing of file descriptor 0 after file-descriptor exhaustion.	4.8	More Details
CVE-2021-24963	The LiteSpeed Cache WordPress plugin before 4.4.4 does not escape the qc_res parameter before outputting it back in the JS code of an admin page, leading to a Reflected Cross-Site Scripting	4.8	More Details
CVE-2021-24991	The WooCommerce PDF Invoices & Packing Slips WordPress plugin before 2.10.5 does not escape the tab and section parameters before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting in the admin dashboard	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20870	Improper handling of exceptional conditions vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, bizhub 4752/4052 GC9-X4 and earlier, bizhub C3850/C3350/3850FS, bizhub 4750/4050, bizhub C3110, bizhub C3100P) allows a physical attacker to obtain unsent scanned image data when scanned data transmission is stopped due to the network error by ejecting a HDD before the scan job times out.	4.6	More Details
CVE-2021-20868	Incorrect authorization vulnerability in KONICA MINOLTA bizhub series (bizhub C750i G00-35 and earlier, bizhub C650i/C550i/C450i G00-B6 and earlier, bizhub C360i/C300i/C250i G00-B6 and earlier, bizhub 750i/650i/550i/450i G00-37 and earlier, bizhub 360i/300i G00-33 and earlier, bizhub C287i/C257i/C227i G00-19 and earlier, bizhub 306i/266i/246i/226i G00-B6 and earlier, bizhub C759/C659 GC7-X8 and earlier, bizhub C658/C558/C458 GC7-X8 and earlier, bizhub 958/808/758 GC7-X8 and earlier, bizhub 658e/558e/458e GC7-X8 and earlier, bizhub C287/C227 GC7-X8 and earlier, bizhub 287/227 GC7-X8 and earlier, bizhub 368e/308e GC7-X8 and earlier, bizhub C368/C308/C258 GC9-X4 and earlier, bizhub 558/458/368/308 GC9-X4 and earlier, bizhub C754e/C654e GDQ-M0 and earlier, bizhub 754e/654e GDQ-M0 and earlier, bizhub C554e/C454e GDQ-M1 and earlier, bizhub C364e/C284e/C224e GDQ-M1 and earlier, bizhub 554e/454e/364e/284e/224e GDQ-M1 and earlier, bizhub C754/C654 C554/C454 GR1-M0 and earlier, bizhub C364/C284/C224 GR1-M0 and earlier, bizhub 754/654 GR1-M0 and earlier, bizhub C4050i/C3350i/C4000i/C3300i G00-B6 and earlier, bizhub C3320i G00-B6 and earlier, bizhub 4750i/4050i G00-22 and earlier, bizhub 4700i G00-22 and earlier, bizhub C3851FS/C3851/C3351 GC9-X4 and earlier, and bizhub 4752/4052 GC9-X4 and earlier) allows an attacker on the adjacent network to obtain user credentials if external server authentication is enabled via a specific SOAP message sent by an administrative user.	4.5	More Details
CVE-2022-20018	In seninf driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05863018; Issue ID: ALPS05863018.	4.4	More Details
CVE-2022-20015	In kd_camera_hw driver, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862966; Issue ID: ALPS05862966.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20148	ManageEngine ADSelfService Plus below build 6116 stores the password policy file for each domain under the html/ web root with a predictable filename based on the domain name. When ADSSP is configured with multiple Windows domains, a user from one domain can obtain the password policy for another domain by authenticating to the service and then sending a request specifying the password policy file of the other domain.	4.3	More Details
CVE-2021-36751	ENC DataVault 7.2.3 and before, and OEM versions, use an encryption algorithm that is vulnerable to data manipulation (without knowledge of the key). This is called ciphertext malleability. There is no data integrity mechanism to detect this manipulation.	4.2	More Details
CVE-2021-43862	jQuery Terminal Emulator is a plugin for creating command line interpreters in your applications. Versions prior to 2.31.1 contain a low impact and limited cross-site scripting (XSS) vulnerability. The code for XSS payload is always visible, but an attacker can use other techniques to hide the code the victim sees. If the application uses the `execHash` option and executes code from URL, the attacker can use this URL to execute their code. The scope is limited because the javascript attribute used is added to span tag, so no automatic execution like with `onerror` on images is possible. This issue is fixed in version 2.31.1. As a workaround, the user can use formatting that wrap whole user input and its no op. The code for this workaround is available in the GitHub Security Advisory. The fix will only work when user of the library is not using different formatters (e.g. to highlight code in different way).	3.7	More Details
CVE-2021-45916	The programming function of Shockwall system has an improper input validation vulnerability. An authenticated attacker within the local area network can send malicious response to the server to disrupt the service partially.	3.5	More Details
CVE-2021-44168	A download of code without integrity check vulnerability in the "execute restore src-vis" command of FortiOS before 7.0.3 may allow a local authenticated attacker to download arbitrary files on the device via specially crafted update packages.	3.3	More Details
CVE-2021-45945	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-41610	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-27339. Reason: This candidate is a reservation duplicate of CVE-2020-27339. Notes: All CVE users should reference CVE-2020-27339 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-45959	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-45817	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-11689. Reason: This candidate is a duplicate of CVE-2018-11689. Notes: All CVE users should reference CVE-2018-11689 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details