SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 30 December 2020

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-26282	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.	10.0	More Details
CVE-2020-25153	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.	9.8	More Details
CVE-2020-28276	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35244	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::addGroup.	9.8	More Details
CVE-2020-35245	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::addUser.	9.8	More Details
CVE-2020-35729	KLog Server 2.4.1 allows OS command injection via shell metacharacters in the actions/authenticate.php user parameter.	9.8	More Details
CVE-2020-26030	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.	9.8	More Details
CVE-2020-35613	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.	9.8	More Details
CVE-2020-27172	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 to elevation of privileges.	9.8	More Details
CVE-2020-35769	miniserv.pl in Webmin 1.962 on Windows mishandles special characters in query arguments to the CGI program.	9.8	More Details
CVE-2020-28277	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.	9.8	More Details
CVE-2020-25196	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 attacks to bypass authentication.	9.8	More Details
CVE-2020-28278	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.	9.8	More Details
CVE-2020-28279	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28280	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.	9.8	More Details
CVE-2020-28281	Prototype pollution vulnerability in 'set-object-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.	9.8	More Details
CVE-2020-28282	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.	9.8	More Details
CVE-2020-28283	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.	9.8	More Details
CVE-2020-10148	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. SolarWinds Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1 are affected.	9.8	More Details
CVE-2020-10207	Use of Hard-coded Credentials in EntoneWebEngine in Amino Communications AK45x series, AK5xx series, AK65x series, Aria6xx series, Aria7/AK7Xx series and Kami7B allows remote attackers to retrieve and modify the device settings.	9.8	More Details
CVE-2020-35243	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::updateUserInfoInDb.	9.8	More Details
CVE-2020-35242	Flamingo (aka FlamingoIM) through 2020-09-29 has a SQL injection vulnerability in UserManager::updateUserTeamInfoInDbAndMemory.	9.8	More Details
CVE-2020-29203	struct2json before 2020-11-18 is affected by a Buffer Overflow because strcpy is used for S2J_STRUCT_GET_string_ELEMENT.	9.8	More Details
CVE-2020-35364	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11720	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.	9.8	More Details
CVE-2020-29552	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.	9.8	More Details
CVE-2020-13968	CRK Business Platform <= 2019.1 allows can inject SQL statements against the DB on any path using the 'strSessao' parameter.	9.8	More Details
CVE-2020-28070	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.	9.8	More Details
CVE-2020-28073	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.	9.8	More Details
CVE-2020-28074	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.	9.8	More Details
CVE-2020-35665	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.	9.8	More Details
CVE-2020-10210	Because of hard-coded SSH keys for the root user in Amino Communications AK45x series, AK5xx series, AK65x series, Aria6xx series, Aria7/AK7Xx series, Kami7B, an attacker may remotely log in through SSH.	9.8	More Details
CVE-2020-28187	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.	9.8	More Details
CVE-2020-28188	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29472	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.	9.8	More Details
CVE-2020-29474	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.	9.8	More Details
CVE-2020-35712	Esri ArcGIS Server before 10.8 is vulnerable to SSRF in some configurations.	9.8	More Details
CVE-2020-35713	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.	9.8	More Details
CVE-2020-35575	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.	9.8	More Details
CVE-2020-26290	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).	9.3	More Details
CVE-2020-29551	An issue was discovered in URVE Build 24.03.2020. Using the _internal/pc/shutdown.php 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.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2503	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.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-27645	The Inventory module of the 1E Client 5.0.0.745 doesn't handle an unquoted path when executing %PROGRAMFILES%\1E\Client\Tachyon.Performance.Metrics.exe. This may allow remote authenticated users and local users to gain elevated privileges.	8.8	More Details
CVE-2020-35773	The site-offline plugin before 1.4.4 for WordPress lacks certain wp_create_nonce and wp_verify_nonce calls, aka CSRF.	8.8	More Details
CVE-2020-35714	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.	8.8	More Details
CVE-2020-25917	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.	8.8	More Details
CVE-2020-26766	A Cross Site Request Forgery (CSRF) vulnerability exists in the loginsystem page in PHPGurukul User Registration & Login and User Management System With Admin Panel 2.1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35693	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 S5.	8.8	More Details
CVE-2020-35627	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 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.	8.8	More Details
CVE-2020-25847	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.	8.8	More Details
CVE-2020-35666	Steedos Platform through 1.21.24 allows NoSQL injection because the /api/collection/findone implementation in server/packages/steedos_base.js mishandles req.body validation, as demonstrated by MongoDB operator attacks such as an X-User-Id[$ne]=1 value.	8.8	More Details
CVE-2020-35370	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.	8.8	More Details
CVE-2020-35269	Nagios Core application version 4.2.4 is vulnerable to Site-Wide Cross-Site Request Forgery (CSRF) in many functions, like adding – deleting for hosts or servers.	8.8	More Details
CVE-2020-27397	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35715	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.	8.8	More Details
CVE-2020-25198	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.	8.8	More Details
CVE-2020-27644	The Inventory module of the 1E Client 5.0.0.745 doesn't handle an unquoted path when executing %PROGRAMFILES%\1E\Client\Tachyon.Performance.Metrics.exe. This may allow remote authenticated users and local users to gain elevated privileges by placing a malicious cryptbase.dll file in %WINDIR%\Temp\.	8.8	More Details
CVE-2020-25194	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.	8.8	More Details
CVE-2020-16268	The MSI installer in 1E Client 4.1.0.267 and 5.0.0.745 allows remote authenticated users and local users to gain elevated privileges via the repair option. This applies to installations that have a TRANSFORM (MST) with the option to disable the installation of the Nomad module. An attacker may craft a .reg file in a specific location that will be able to write to any registry key as an elevated user.	8.8	More Details
CVE-2020-26287	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 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.	8.7	More Details
CVE-2020-35728	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).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17533	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.	8.1	More Details
CVE-2020-7845	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.	8.1	More Details
CVE-2020-29189	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	8.1	More Details
CVE-2020-35766	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.	7.8	More Details
CVE-2020-35702	DCTStream::getChars in 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	7.8	More Details
CVE-2020-8289	Backblaze for Windows before 7.0.1.433 and Backblaze for macOS before 7.0.1.434 suffer from improper certificate 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.	7.8	More Details
CVE-2020-9200	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.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25507	An incorrect permission assignment during the installation script of TeamworkCloud 18.0 thru 19.0 allows a local unprivileged attacker to execute arbitrary code as root. During installation, the user is instructed to set the system enviroment file with world writable permissions (0777 /etc/environment). Any local unprivileged user can execute arbitrary code simply by writing to /etc/environment, which will force all users, including root, to execute arbitrary code during the next login or reboot. In addition, the entire home directory of the twcloud user at /home/twcloud is recursively given world writable permissions. This allows any local unprivileged attacker to execute arbitrary code, as twcloud. This product was previous named Cameo Enterprise Data Warehouse (CEDW).	7.8	More Details
CVE-2020-8290	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.	7.8	More Details
CVE-2020-9207	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.	7.8	More Details
CVE-2020-24658	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 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).	7.8	More Details
CVE-2020-5681	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.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35679	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.	7.5	More Details
CVE-2020-35736	GateOne 1.1 allows arbitrary file download without authentication via /downloads/.. directory traversal because os.path.join is misused.	7.5	More Details
CVE-2020-27728	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.	7.5	More Details
CVE-2020-28094	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.	7.5	More Details
CVE-2020-27723	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.	7.5	More Details
CVE-2020-29194	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.	7.5	More Details
CVE-2020-27720	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 undisclosed traffic pattern may cause the Traffic Management Microkernel (TMM) to restart.	7.5	More Details
CVE-2020-35680	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 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.	7.5	More Details
CVE-2020-35587	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	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9120	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.	7.5	More Details
CVE-2020-27717	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.	7.5	More Details
CVE-2020-11093	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 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.	7.5	More Details
CVE-2020-35362	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).	7.5	More Details
CVE-2020-35284	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 the product's source code is available.	7.5	More Details
CVE-2020-35450	Gobby 0.4.11 allows a NULL pointer dereference in the D-Bus handler for certain set_language calls.	7.5	More Details
CVE-2020-35359	Pure-FTPd 1.0.48 allows remote attackers to prevent legitimate server use by making enough connections to exceed the connection limit.	7.5	More Details
CVE-2020-35376	Xpdf 4.02 allows stack consumption because of an incorrect subroutine reference in a Type 1C font charstring, related to the FoFiType1C::getOp() function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35388	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.	7.5	More Details
CVE-2020-25190	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.	7.5	More Details
CVE-2020-35711	An issue has been discovered in the arc-swap crate before 0.4.8 (and 1.x before 1.1.0) for Rust. Use 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.	7.5	More Details
CVE-2020-26032	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.	7.5	More Details
CVE-2020-27714	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-TCP traffic.	7.5	More Details
CVE-2020-27716	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.	7.5	More Details
CVE-2020-26286	HedgeDoc is a collaborative platform for writing and sharing markdown. In HedgeDoc before version 1.7.1 an 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.	7.5	More Details
CVE-2020-9094	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29550	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/000000010000000A000000DD, 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.	7.5	More Details
CVE-2018-1000891	Bitcoin SV before 0.1.1 allows uncontrolled resource consumption when receiving messages with invalid checksums.	7.5	More Details
CVE-2018-1000892	Bitcoin SV before 0.1.1 allows uncontrolled resource consumption when receiving sendheaders messages.	7.5	More Details
CVE-2018-1000893	Bitcoin SV before 0.1.1 allows uncontrolled resource consumption when deserializing transactions.	7.5	More Details
CVE-2020-11719	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.	7.5	More Details
CVE-2020-5807	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.	7.5	More Details
CVE-2020-5802	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5801	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.	7.5	More Details
CVE-2020-35586	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).	7.5	More Details
CVE-2020-35585	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.	7.5	More Details
CVE-2020-35598	ACS Advanced Comment System 1.0 is affected by Directory Traversal via an advanced_component_system/index.php?ACS_path=..%2f URI. NOTE: this might be the same as CVE-2009-4623	7.5	More Details
CVE-2020-35668	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.	7.5	More Details
CVE-2020-27715	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.	7.5	More Details
CVE-2020-9223	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.	7.5	More Details
CVE-2020-35616	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.	7.5	More Details
CVE-2020-35612	An issue was discovered in Joomla! 2.5.0 through 3.9.22. The folder parameter of mod_random_image lacked input validation, leading to a path traversal vulnerability.	7.5	More Details
CVE-2020-9124	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29160	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.	7.5	More Details
CVE-2020-26289	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.	7.5	More Details
CVE-2020-35716	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.	7.5	More Details
CVE-2020-35610	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.	7.5	More Details
CVE-2020-27721	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.	7.5	More Details
CVE-2020-27718	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.	7.5	More Details
CVE-2020-35611	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.	7.5	More Details
CVE-2020-14273	HCL Domino 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.	7.5	More Details
CVE-2020-11718	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.	7.4	More Details
CVE-2020-24360	An issue with ARP packets in Arista's EOS affecting the 7800R3, 7500R3, and 7280R3 series of products may result in issues that cause a kernel crash, followed by a device reload. The affected Arista EOS versions are: 4.24.2.4F and below releases in the 4.24.x train; 4.23.4M and below releases in the 4.23.x train; 4.22.6M and below releases in the 4.22.x train.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28186	Email Injection in TerraMaster TOS <= 4.2.06 allows remote unauthenticated attackers to abuse the forget password functionality and achieve account takeover.	7.3	More Details
CVE-2020-29299	Certain Zyxel products allow command injection by an admin via an input string to chg_exp_pwd during a password-change action. This affects VPN On-premise before ZLD V4.39 week38, VPN Orchestrator before SD-OS V10.03 week32, USG before ZLD V4.39 week38, USG FLEX before ZLD V4.55 week38, ATP before ZLD V4.55 week38, and NSG before 1.33 patch 4.	7.2	More Details
CVE-2020-28093	On Tenda AC1200 (Model AC6) 15.03.06.51_multi devices, admin, support, user, and nobody have a password of 1234.	7.2	More Details
CVE-2020-35657	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 Job Access With Speech) product.	7.2	More Details
CVE-2020-35656	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.	7.2	More Details
CVE-2020-35708	phpList 3.5.9 allows SQL injection by admins who provide a crafted fourth line of a file to the "Config - Import Administrators" page.	7.2	More Details
CVE-2020-35136	Dolibarr 12.0.3 is vulnerable to authenticated Remote Code Execution. An 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.	7.2	More Details
CVE-2020-28169	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.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28912	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.	7.0	More Details
CVE-2020-29193	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).	6.8	More Details
CVE-2020-28096	FOSCAM FHD X1 1.14.2.4 devices allow attackers (with physical UART access) to login via the ipc.fos~ password.	6.8	More Details
CVE-2020-9125	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.	6.7	More Details
CVE-2020-9137	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.	6.7	More Details
CVE-2020-13474	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.	6.5	More Details
CVE-2020-26029	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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29242	dhowden tag before 2020-11-19 allows "panic: runtime error: index out of range" via readPICFrame.	6.5	More Details
CVE-2020-29243	dhowden tag before 2020-11-19 allows "panic: runtime error: index out of range" via readAPICFrame.	6.5	More Details
CVE-2020-29245	dhowden tag before 2020-11-19 allows "panic: runtime error: slice bounds out of range" via readAtomData.	6.5	More Details
CVE-2020-27724	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.	6.5	More Details
CVE-2020-9201	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.	6.5	More Details
CVE-2020-27722	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, under certain conditions, the VDI plugin does not observe plugin flow-control protocol causing excessive resource consumption.	6.5	More Details
CVE-2020-29244	dhowden tag before 2020-11-19 allows "panic: runtime error: slice bounds out of range" via readTextWithDescrFrame.	6.5	More Details
CVE-2020-27643	The %PROGRAMDATA%\1E\Client directory in 1E Client 5.0.0.745 and 4.1.0.267 allows remote authenticated users and local users to create and modify files in protected directories (where they would not normally have access to create or modify files) via the creation of a junction point to a system directory. This leads to partial privilege escalation.	6.5	More Details
CVE-2020-9208	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 to information leak.	6.5	More Details
CVE-2020-20412	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. NOTE: this may overlap CVE-2018-5146.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35347	CXUUCMS V3 3.1 has a CSRF vulnerability that can add an administrator account via admin.php?c=adminuser&a=add.	6.5	More Details
CVE-2020-27837	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.	6.4	More Details
CVE-2020-2499	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.	6.3	More Details
CVE-2020-35615	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.	6.3	More Details
CVE-2020-9119	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.	6.2	More Details
CVE-2020-35650	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 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-uo_groups.php, or the message GET Parameter in frontend-uo_groups.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27719	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.	6.1	More Details
CVE-2020-6159	URLs using “javascript:” have the protocol removed when pasted into the address bar to protect users from cross-site scripting (XSS) attacks, but 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.	6.1	More Details
CVE-2020-35669	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.	6.1	More Details
CVE-2020-9439	Multiple cross-site scripting (XSS) vulnerabilities in Uncanny Owl Tin Canny LearnDash Reporting before 3.4.4 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.	6.1	More Details
CVE-2020-35676	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 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.	6.1	More Details
CVE-2020-13969	CRK Business Platform <= 2019.1 allows reflected XSS via erro.aspx on 'CRK', 'IDContratante', 'Erro', or 'Mod' parameter. This is path-independent.	6.1	More Details
CVE-2020-35252	Cross Site Scripting (XSS) vulnerability via the 'Full Name' parameter in the User Registration section of User Registration & Login System with Admin Panel 1.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35730	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.	6.1	More Details
CVE-2020-29172	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.	6.1	More Details
CVE-2020-27726	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 configured on the BIG-IP APM system.	6.1	More Details
CVE-2020-27729	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.	6.1	More Details
CVE-2020-35678	AutobahnIPython before 20.12.3 allows redirect header injection.	6.1	More Details
CVE-2020-27515	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.	6.1	More Details
CVE-2020-29204	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.	6.1	More Details
CVE-2020-35659	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.	6.1	More Details
CVE-2020-29249	CXUUCMS V3 allows class="layui-input" XSS.	6.1	More Details
CVE-2020-29250	CXUUCMS V3 allows XSS via the first and third input fields to /public/admin.php.	6.1	More Details
CVE-2020-35437	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.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35738	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.	6.1	More Details
CVE-2020-35584	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.	5.9	More Details
CVE-2020-26569	In EVPN VxLAN setups in Arista EOS, specific malformed packets can lead to incorrect MAC to IP bindings and as a result packets can be incorrectly forwarded across VLAN boundaries. This can result in traffic being discarded on the receiving VLAN. This affects versions: 4.21.12M and below releases in the 4.21.x train; 4.22.7M and below releases in the 4.22.x train; 4.23.5M and below releases in the 4.23.x train; 4.24.2F and below releases in the 4.24.x train.	5.9	More Details
CVE-2020-28190	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.	5.9	More Details
CVE-2020-2504	If exploited, this absolute path traversal vulnerability could allow attackers to traverse files in File Station. QNAP has already fixed these issues in QES 2.1.1 Build 20201006 and later.	5.8	More Details
CVE-2020-29385	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.	5.5	More Details
CVE-2020-5806	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 specially crafted message to 127.0.0.1:7153. Observed in FactoryTalk Linx 6.11. All versions of FactoryTalk Linx are affected.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4642	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".	5.5	More Details
CVE-2020-1848	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.	5.5	More Details
CVE-2020-28759	The serializer module in OAID Tengine lite-v1.0 has a Buffer Overflow and crash. NOTE: another person has stated "I don't think there is an proof of overflow so far.	5.5	More Details
CVE-2020-9093	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.	5.5	More Details
CVE-2020-13473	NCH Express Accounts 8.24 and earlier allows local users to discover the cleartext password by reading the configuration file.	5.5	More Details
CVE-2020-28184	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.	5.4	More Details
CVE-2020-35707	Daybyday 2.1.0 allows stored XSS via the Company Name parameter to the New Client screen.	5.4	More Details
CVE-2020-26035	An issue was discovered in Zammad before 3.4.1. There is Stored XSS via a Tags element in a TIcket.	5.4	More Details
CVE-2020-35706	Daybyday 2.1.0 allows stored XSS via the Title parameter to the New Project screen.	5.4	More Details
CVE-2020-35774	server/handler/HistogramQueryHandler.scala in Twitter TwitterServer (aka twitter-server) before 20.12.0, in some configurations, allows XSS via the /histograms endpoint.	5.4	More Details
CVE-2020-26033	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.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35705	Daybyday 2.1.0 allows stored XSS via the Name parameter to the New User screen.	5.4	More Details
CVE-2020-35704	Daybyday 2.1.0 allows stored XSS via the Title parameter to the New Lead screen.	5.4	More Details
CVE-2020-25192	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.	5.3	More Details
CVE-2020-35658	SpamTitan before 7.09 allows attackers to tamper with backups, because backups are not encrypted.	5.3	More Details
CVE-2020-35710	Parallels Remote Application Server (RAS) 18 allows remote attackers to discover an intranet IP address because submission of the login 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.	5.3	More Details
CVE-2020-28185	User Enumeration vulnerability in TerraMaster TOS <= 4.2.06 allows remote unauthenticated attackers to identify valid users within the system via the username parameter to wizard/initialise.php.	5.3	More Details
CVE-2020-35614	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.	5.3	More Details
CVE-2020-29156	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.	5.3	More Details
CVE-2020-15898	In Arista EOS malformed packets can be incorrectly forwarded across VLAN boundaries in one direction. This vulnerability is only susceptible to exploitation by unidirectional traffic (ex. UDP) and not bidirectional traffic (ex. TCP). This affects: EOS 7170 platforms version 4.21.4.1F and below releases in the 4.21.x train; EOS X-Series versions 4.21.11M and below releases in the 4.21.x train; 4.22.6M and below releases in the 4.22.x train; 4.23.4M and below releases in the 4.23.x train; 4.24.2.1F and below releases in the 4.24.x train.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27727	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.	4.9	More Details
CVE-2020-29159	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.	4.9	More Details
CVE-2020-35709	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.	4.9	More Details
CVE-2020-26028	An issue was discovered in Zammad before 3.4.1. Admin Users without a ticket.* permission can access Tickets.	4.9	More Details
CVE-2020-35349	Savsoft Quiz 5 is affected by: Cross Site Scripting (XSS) via field_title (aka a title on the custom fields page).	4.8	More Details
CVE-2020-28071	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.	4.8	More Details
CVE-2020-5684	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.	4.8	More Details
CVE-2020-29247	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.	4.8	More Details
CVE-2020-35346	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.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35677	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.	4.8	More Details
CVE-2020-29475	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.	4.8	More Details
CVE-2020-13476	NCH Express Invoice 8.06 to 8.24 is vulnerable to Reflected XSS in the Quotes List module.	4.8	More Details
CVE-2020-29471	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.	4.8	More Details
CVE-2020-29470	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.	4.8	More Details
CVE-2020-35735	Vidyo 02-09-/D allows clickjacking via the portal/ URI.	4.7	More Details
CVE-2020-9202	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.	4.4	More Details
CVE-2020-27725	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.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29158	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.	4.3	More Details
CVE-2020-26034	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.	4.3	More Details
CVE-2020-26031	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).	4.3	More Details
CVE-2020-35448	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.	3.3	More Details
CVE-2020-2505	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.	2.3	More Details
CVE-2020-28189	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-29189. Reason: This candidate is a reservation duplicate of CVE-2020-29189. Notes: All CVE users should reference CVE-2020-29189 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-28275	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