SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 07 October 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-2020-7741	This affects the package hellojs before 1.18.6. The code get the param oauth_redirect from url and pass it to location.assign without any check and sanitisation. So we can simply pass some XSS payloads into the url param oauth_redirect, such as javascript:alert(1).	9.9	More Details
CVE-2020-12125	A remote buffer overflow vulnerability in the /cgi-bin/makeRequest.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to execute arbitrary machine instructions as root without authentication.	9.8	More Details
CVE-2020-24231	Symmetric DS <3.12.0 uses mx4j to provide access to JMX over HTTP. mx4j, by default, has no auth and is available on all interfaces. An attacker can interact with JMX: get system info, and invoke MBean methods. It is possible to install additional MBeans from a remote host using MLet that leads to arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12124	A remote command-line injection vulnerability in the /cgi-bin/live_api.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to execute arbitrary Linux commands as root without authentication.	9.8	More Details
CVE-2018-5353	The custom GINA/CP module in Zoho ManageEngine ADSelfService Plus before 5.5 build 5517 allows remote attackers to execute code and escalate privileges via spoofing. It does not authenticate the intended server before opening a browser window. An unauthenticated attacker capable of conducting a spoofing attack can redirect the browser to gain execution in the context of the WinLogon.exe process. If Network Level Authentication is not enforced, the vulnerability can be exploited via RDP. Additionally, if the web server has a misconfigured certificate then no spoofing attack is required	9.8	More Details
CVE-2020-12126	Multiple authentication bypass vulnerabilities in the /cgi-bin/ endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allow an attacker to leak router settings, change configuration variables, and cause denial of service via an unauthenticated endpoint.	9.8	More Details
CVE-2020-24698	An issue was discovered in PowerDNS Authoritative through 4.3.0 when --enable-experimental-gss-tsig is used. A remote, unauthenticated attacker might be able to cause a double-free, leading to a crash or possibly arbitrary code execution. by sending crafted queries with a GSS-TSIG signature.	9.8	More Details
CVE-2020-18185	class.plx.admin.php in PluXml 5.7 allows attackers to execute arbitrary PHP code by modify the configuration file in a linux environment.	9.8	More Details
CVE-2020-26527	An issue was discovered in API/api/Version in Damstra Smart Asset 2020.7. Cross-origin resource sharing trusts random origins by accepting the arbitrary 'Origin: example.com' header and responding with 200 OK and a wildcard 'Access-Control-Allow-Origin: *' header.	9.8	More Details
CVE-2020-4493	IBM Maximo Asset Management 7.6.0 and 7.6.1 could allow an attacker to bypass authentication and issue commands using a specially crafted HTTP command. IBM X-Force ID: 181995.	9.8	More Details
CVE-2020-6875	A ZTE product is impacted by the improper access control vulnerability. Due to lack of an authentication protection mechanism in the program, attackers could use this vulnerability to gain access right through brute-force attacks. This affects: <ZXONE 19700 SNPE> <ZXONE8700V1.40R2B13_SNPE>	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16226	Multiple Mitsubishi Electric products are vulnerable to impersonations of a legitimate device by a malicious actor, which may allow an attacker to remotely execute arbitrary commands.	9.8	More Details
CVE-2020-26537	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. In a certain Shading calculation, the number of outputs is unequal to the number of color components in a color space. This causes an out-of-bounds write.	9.8	More Details
CVE-1999-0199	manual/search.texi in the GNU C Library (aka glibc) before 2.2 lacks a statement about the unspecified tdelete return value upon deletion of a tree's root, which might allow attackers to access a dangling pointer in an application whose developer was unaware of a documentation update from 1999.	9.8	More Details
CVE-2020-24214	An issue was discovered in the box application on HiSilicon based IPTV/H.264/H.265 video encoders. Attackers can send a crafted unauthenticated RTSP request to cause a buffer overflow and application crash. The device will not be able to perform its main purpose of video encoding and streaming for up to a minute, until it automatically reboots. Attackers can send malicious requests once a minute, effectively disabling the device.	9.8	More Details
CVE-2020-24215	An issue was discovered in the box application on HiSilicon based IPTV/H.264/H.265 video encoders. Attackers can use hard-coded credentials in HTTP requests to perform any administrative task on the device including retrieving the device's configuration (with the cleartext admin password), and uploading a custom firmware update, to ultimately achieve arbitrary code execution.	9.8	More Details
CVE-2020-24217	An issue was discovered in the box application on HiSilicon based IPTV/H.264/H.265 video encoders. The file-upload endpoint does not enforce authentication. Attackers can send an unauthenticated HTTP request to upload a custom firmware component, possibly in conjunction with command injection, to achieve arbitrary code execution.	9.8	More Details
CVE-2020-24218	An issue was discovered on URayTech IPTV/H.264/H.265 video encoders through 1.97. Attackers can log in as root via the password that is hard-coded in the executable file.	9.8	More Details
CVE-2020-7465	The L2TP implementation of MPD before 5.9 allows a remote attacker who can send specifically crafted L2TP control packet with AVP Q.931 Cause Code to execute arbitrary code or cause a denial of service (memory corruption).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1907	A stack overflow in WhatsApp for Android prior to v2.20.196.16, WhatsApp Business for Android prior to v2.20.196.12, WhatsApp for iOS prior to v2.20.90, WhatsApp Business for iOS prior to v2.20.90, and WhatsApp for Portal prior to v173.0.0.29.505 could have allowed arbitrary code execution when parsing the contents of an RTP Extension header.	9.8	More Details
CVE-2020-26539	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. When there is a multiple interpretation error for /V (in the Additional Action and Field dictionaries), a use-after-free can occur with resultant remote code execution (or an information leak).	9.8	More Details
CVE-2020-26607	An issue was discovered in TimaService on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. PendingIntent with an empty intent is mishandled, allowing an attacker to perform a privileged action via a modified intent. The Samsung ID is SVE-2020-18418 (October 2020).	9.8	More Details
CVE-2020-26535	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. If TslAlloc attempts to allocate thread local storage but obtains an unacceptable index value, V8 throws an exception that leads to a write access violation (and read access violation).	9.8	More Details
CVE-2020-26534	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. There is an Opt object use-after-free related to Field::ClearItems and Field::DeleteOptions, during AcroForm JavaScript execution.	9.8	More Details
CVE-2020-15487	Re:Desk 2.3 contains a blind unauthenticated SQL injection vulnerability in the getBaseCriteria() function in the protected/models/Ticket.php file. By modifying the folder GET parameter, it is possible to execute arbitrary SQL statements via a crafted URL. Unauthenticated remote command execution is possible by using this SQL injection to update certain database values, which are then executed by a bizRule eval() function in the yii/framework/web/auth/CAuthManager.php file. Resultant authorization bypass is also possible, by recovering or modifying password hashes and password reset tokens, allowing for administrative privileges to be obtained.	9.8	More Details
CVE-2020-19672	Niushop B2B2C Multi-business basic version V1.11, can bypass the administrator to obtain the background upload interface, through parameter upload, bypass the getimagesize function, upload php file, getshell.	9.8	More Details
CVE-2020-20800	An issue was discovered in MetInfo v7.0.0 beta. There is SQL Injection via the install/index.php?action=adminsetup&cndata=yes&endata=yes&showdata=yes URI.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21522	An issue was discovered in halo V1.1.3. A Zip Slip Directory Traversal Vulnerability in the backend,the attacker can overwrite some files, such as ftl files, .bashrc files in the user directory, and finally get the permissions of the operating system.	9.8	More Details
CVE-2020-21523	A Server-Side Freemarker template injection vulnerability in halo CMS v1.1.3 In the Edit Theme File function. The ftl file can be edited. This is the Freemarker template file. This file can cause arbitrary code execution when it is rendered in the background. exp: <#assign test="freemarker.template.utility.Execute"?new()> ${test("touch /tmp/freemarkerPwned")}	9.8	More Details
CVE-2020-21526	An Arbitrary file writing vulnerability in halo v1.1.3. In an interface to write files in the background, a directory traversal check is performed on the input path parameter, but the startsWith function can be used to bypass it.	9.8	More Details
CVE-2020-25763	Seat Reservation System version 1.0 suffers from an Unauthenticated File Upload Vulnerability allowing Remote Attackers to gain Remote Code Execution (RCE) on the Hosting Webserver via uploading PHP files.	9.8	More Details
CVE-2020-26041	An issue was discovered in Hoosk CmS v1.8.0. There is an Remote Code Execution vulnerability in install/index.php	9.8	More Details
CVE-2020-26042	An issue was discovered in Hoosk CMS v1.8.0. There is a SQL injection vulnerability in install/index.php	9.8	More Details
CVE-2020-26154	url.cpp in libproxy through 0.4.15 is prone to a buffer overflow when PAC is enabled, as demonstrated by a large PAC file that is delivered without a Content-length header.	9.8	More Details
CVE-2020-12870	RainbowFish PacsOne Server 6.8.4 allows SQL injection on the username parameter in the signup page.	9.8	More Details
CVE-2020-25990	WebsiteBaker 2.12.2 allows SQL Injection via parameter 'display_name' in /websitebaker/admin/preferences/save.php. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	9.8	More Details
CVE-2020-15533	In Zoho ManageEngine Application Manager 14.7 Build 14730 (before 14684, and between 14689 and 14750), the AlarmEscalation module is vulnerable to unauthenticated SQL Injection attack.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26518	Artica Pandora FMS before 743 allows unauthenticated attackers to conduct SQL injection attacks via the pandora_console/include/chart_generator.php session_id parameter.	9.8	More Details
CVE-2020-26157	Leanote Desktop through 2.6.2 allows XSS because a note's title is mishandled during syncing. This leads to remote code execution because of Node integration.	9.6	More Details
CVE-2020-26158	Leanote Desktop through 2.6.2 allows XSS because a note's title is mishandled when the batch feature is triggered. This leads to remote code execution because of Node integration.	9.6	More Details
CVE-2020-26574	Leostream Connection Broker 8.2.x is affected by stored XSS. An unauthenticated attacker can inject arbitrary JavaScript code via the webquery.pl User-Agent HTTP header. It is rendered by the admins the next time they log in. The JavaScript injected can be used to force the admin to upload a malicious Perl script that will be executed as root via libMisc::browser_client. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.6	More Details
CVE-2020-15232	In mapfish-print before version 3.24, a user can do to an XML External Entity (XXE) attack with the provided SDL style.	9.3	More Details
CVE-2020-15231	In mapfish-print before version 3.24, a user can use the JSONP support to do a Cross-site scripting.	9.3	More Details
CVE-2020-26525	Damstra Smart Asset 2020.7 has SQL injection via the API/api/Asset originator parameter. This allows forcing the database and server to initiate remote connections to third party DNS servers.	9.1	More Details
CVE-2020-12676	FusionAuth fusionauth-samlv2 0.2.3 allows remote attackers to forge messages and bypass authentication via a SAML assertion that lacks a Signature element, aka a "Signature exclusion attack".	9.1	More Details
CVE-2020-18191	GetSimpleCMS-3.3.15 is affected by directory traversal. Remote attackers are able to delete arbitrary files via /GetSimpleCMS-3.3.15/admin/log.php	9.1	More Details
CVE-2020-25762	An issue was discovered in SourceCodester Seat Reservation System 1.0. The file admin_class.php does not perform input validation on the username and password parameters. An attacker can send malicious input in the post request to /admin/ajax.php?action=login and bypass authentication, extract sensitive information etc.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-18190	Bludit v3.8.1 is affected by directory traversal. Remote attackers are able to delete arbitrary files via /admin/ajax/upload-profile-picture.	9.1	More Details
CVE-2020-21524	There is a XML external entity (XXE) vulnerability in halo v1.1.3, The function of importing other blogs in the background(/api/admin/migrations/wordpress) needs to parse the xml file, but it is not used for security defense, This vulnerability can detect the intranet, read files, enable ddos attacks, etc. exp:https://github.com/halo-dev/halo/issues/423	9.1	More Details
CVE-2020-12506	Improper Authentication vulnerability in WAGO 750-8XX series with FW version <= FW03 allows an attacker to change the settings of the devices by sending specifically constructed requests without authentication This issue affects: WAGO 750-362, WAGO 750-363, WAGO 750-823, WAGO 750-832/xxx-xxx, WAGO 750-862, WAGO 750-891, WAGO 750-890/xxx-xxx in versions FW03 and prior versions.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-15678	When recursing through graphical layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.	8.8	More Details
CVE-2020-15674	Mozilla developers reported memory safety bugs present in Firefox 80. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81.	8.8	More Details
CVE-2020-15927	Zoho ManageEngine Applications Manager version 14740 and prior allows an authenticated SQL Injection via a crafted jsp request in the SAP module.	8.8	More Details
CVE-2019-19200	REDDOXX MailDepot 2032 2.2.1242 allows authenticated users to access the mailboxes of other users.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-21564	An issue was discovered in Pluck CMS 4.7.10-dev2 and 4.7.11. There is a file upload vulnerability that can cause a remote command execution via admin.php?action=files.	8.8	More Details
CVE-2020-26124	openmediavault before 4.1.36 and 5.x before 5.5.12 allows authenticated PHP code injection attacks, via the sortfield POST parameter of rpc.php, because json_encode_safe is not used in config/databasebackend.inc. Successful exploitation allows arbitrary command execution on the underlying operating system as root.	8.8	More Details
CVE-2020-25760	Projectworlds Visitor Management System in PHP 1.0 allows SQL Injection. The file front.php does not perform input validation on the 'rid' parameter. An attacker can append SQL queries to the input to extract sensitive information from the database.	8.8	More Details
CVE-2020-26163	BigBlueButton Greenlight before 2.5.6 allows HTTP header (Host and Origin) attacks, which can result in Account Takeover if a victim follows a spoofed password-reset link.	8.8	More Details
CVE-2020-14374	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. A flawed bounds checking in the copy_data function leads to a buffer overflow allowing an attacker in a virtual machine to write arbitrary data to any address in the vhost_crypto application. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	8.8	More Details
CVE-2020-5786	Cross-site request forgery in Teltonika firmware TRB2_R_00.02.04.3 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link.	8.8	More Details
CVE-2020-12715	RainbowFish PacsOne Server 6.8.4 has Incorrect Access Control.	8.8	More Details
CVE-2020-24628	A remote code injection vulnerability was discovered in HPE KVM IP Console Switches version(s): G2 4x1Ex32 Prior to 2.8.3.	8.8	More Details
CVE-2020-15675	When processing surfaces, the lifetime may outlive a persistent buffer leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 81.	8.8	More Details
CVE-2020-16267	Zoho ManageEngine Applications Manager version 14740 and prior allows an authenticated SQL Injection via a crafted jsp request in the RCA module.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26048	The file manager option in CuppaCMS before 2019-11-12 allows an authenticated attacker to upload a malicious file within an image extension and through a custom request using the rename function provided by the file manager is able to modify the image extension into PHP resulting in remote arbitrary code execution.	8.8	More Details
CVE-2020-15673	Mozilla developers reported memory safety bugs present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.	8.8	More Details
CVE-2020-15670	Mozilla developers reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 80, Firefox ESR < 78.2, Thunderbird < 78.2, and Firefox for Android < 80.	8.8	More Details
CVE-2020-5634	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors.	8.8	More Details
CVE-2020-15669	When aborting an operation, such as a fetch, an abort signal may be deleted while alerting the objects to be notified. This results in a use-after-free and we presume that with enough effort it could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.12 and Thunderbird < 68.12.	8.8	More Details
CVE-2018-5354	The custom GINA/CP module in ANIXIS Password Reset Client before version 3.22 allows remote attackers to execute code and escalate privileges via spoofing. When the client is configured to use HTTP, it does not authenticate the intended server before opening a browser window. An unauthenticated attacker capable of conducting a spoofing attack can redirect the browser to gain execution in the context of the WinLogon.exe process. If Network Level Authentication is not enforced, the vulnerability can be exploited via RDP.	8.8	More Details
CVE-2020-26582	D-Link DAP-1360U before 3.0.1 devices allow remote authenticated users to execute arbitrary commands via shell metacharacters in the IP JSON value for ping (aka res_config_action=3&res_config_id=18).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15667	When processing a MAR update file, after the signature has been validated, an invalid name length could result in a heap overflow, leading to memory corruption and potentially arbitrary code execution. Within Firefox as released by Mozilla, this issue is only exploitable with the Mozilla-controlled signing key. This vulnerability affects Firefox < 80.	8.8	More Details
CVE-2020-15663	If Firefox is installed to a user-writable directory, the Mozilla Maintenance Service would execute updater.exe from the install location with system privileges. Although the Mozilla Maintenance Service does ensure that updater.exe is signed by Mozilla, the version could have been rolled back to a previous version which would have allowed exploitation of an older bug and arbitrary code execution with System Privileges. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, and Firefox ESR < 78.2.	8.8	More Details
CVE-2020-15227	Nette versions before 2.0.19, 2.1.13, 2.2.10, 2.3.14, 2.4.16, 3.0.6 are vulnerable to an code injection attack by passing specially formed parameters to URL that may possibly leading to RCE. Nette is a PHP/Composer MVC Framework.	8.7	More Details
CVE-2020-15236	In Wiki.js before version 2.5.151, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit 084dcd69d1591586ee4752101e675d5f0ac6dcdc fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any directory traversal (e.g. `..` and `.`) sequences as well as invalid filesystem characters from the path. As a workaround, disable any storage module with local asset caching capabilities such as Local File System and Git.	8.6	More Details
CVE-2020-15230	Vapor is a web framework for Swift. In Vapor before version 4.29.4, Attackers can access data at arbitrary filesystem paths on the same host as an application. Only applications using FileMiddleware are affected. This is fixed in version 4.29.4.	8.5	More Details
CVE-2020-13321	A vulnerability was discovered in GitLab versions prior to 13.1. Username format restrictions could be bypassed allowing for html tags to be added.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7738	All versions of package shiba are vulnerable to Arbitrary Code Execution due to the default usage of the function load() of the package js-yaml instead of its secure replacement , safeLoad().	8.3	More Details
CVE-2020-25017	Envoy through 1.15.0 only considers the first value when multiple header values are present for some HTTP headers. Envoy's setCopy() header map API does not replace all existing occurences of a non-inline header.	8.3	More Details
CVE-2020-7739	This affects all versions of package phantomjs-seo. It is possible for an attacker to craft a url that will be passed to a PhantomJS instance allowing for an SSRF attack.	8.2	More Details
CVE-2020-7740	This affects all versions of package node-pdf-generator. Due to lack of user input validation and sanitization done to the content given to node-pdf-generator, it is possible for an attacker to craft a url that will be passed to an external server allowing an SSRF attack.	8.2	More Details
CVE-2020-12505	Improper Authentication vulnerability in WAGO 750-8XX series with FW version <= FW07 allows an attacker to change some special parameters without authentication. This issue affects: WAGO 750-852, WAGO 750-880/xxx-xxx, WAGO 750-881, WAGO 750-831/xxx-xxx, WAGO 750-882, WAGO 750-885/xxx-xxx, WAGO 750-889 in versions FW07 and below.	8.2	More Details
CVE-2020-15589	A design issue was discovered in GetInternetRequestHandle, InternetSendRequestEx and InternetSendRequestByBitrate in the client side of Zoho ManageEngine Desktop Central 10.0.552.W and Remote Access Plus before 10.1.2119.1. By exploiting this issue, an attacker-controlled server can force the client to skip TLS certificate validation, leading to a man-in-the-middle attack against HTTPS and unauthenticated remote code execution.	8.1	More Details
CVE-2020-24696	An issue was discovered in PowerDNS Authoritative through 4.3.0 when --enable-experimental-gss-tsig is used. A remote, unauthenticated attacker can trigger a race condition leading to a crash, or possibly arbitrary code execution, by sending crafted queries with a GSS-TSIG signature.	8.1	More Details
CVE-2019-20920	Handlebars before 3.0.8 and 4.x before 4.5.3 is vulnerable to Arbitrary Code Execution. The lookup helper fails to properly validate templates, allowing attackers to submit templates that execute arbitrary JavaScript. This can be used to run arbitrary code on a server processing Handlebars templates or in a victim's browser (effectively serving as XSS).	8.1	More Details
CVE-2020-12123	CSRF vulnerabilities in the /cgi-bin/ directory of the WAVLINK WN530H4 M30H4.V5030.190403 allow an attacker to remotely access router endpoints, because these endpoints do not contain CSRF tokens. If a user is authenticated in the router portal, then this attack will work.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13952	In the course of work on the open source project it was discovered that authenticated users running queries against Hive and Presto database engines could access information via a number of templated fields including the contents of query description metadata database, the hashed version of the authenticated users' password, and access to connection information including the plaintext password for the current connection. It would also be possible to run arbitrary methods on the database connection object for the Presto or Hive connection, allowing the user to bypass security controls internal to Superset. This vulnerability is present in every Apache Superset version < 0.37.2.	8.1	More Details
CVE-2020-13658	In Lansweeper 8.0.130.17, the web console is vulnerable to a CSRF attack that would allow a low-level Lansweeper user to elevate their privileges within the application.	8.0	More Details
CVE-2020-8182	Improper access control in Nextcloud Deck 0.8.0 allowed an attacker to reshare boards shared with them with more permissions than they had themselves.	8.0	More Details
CVE-2019-14557	Buffer overflow in BIOS firmware for 8th, 9th, 10th Generation Intel(R) Core(TM), Intel(R) Celeron(R) Processor 4000 & 5000 Series Processors may allow an authenticated user to potentially enable elevation of privilege or denial of service via adjacent access.	8.0	More Details
CVE-2020-5979	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which a user is presented with a dialog box for input by a high-privilege process, which may lead to escalation of privileges.	7.8	More Details
CVE-2020-14376	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. A lack of bounds checking when copying iv_data from the VM guest memory into host memory can lead to a large buffer overflow. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-1906	A buffer overflow in WhatsApp for Android prior to v2.20.130 and WhatsApp Business for Android prior to v2.20.46 could have allowed an out-of-bounds write when processing malformed local videos with E-AC-3 audio streams.	7.8	More Details
CVE-2020-5980	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in multiple components in which a securely loaded system DLL will load its dependencies in an insecure fashion, which may lead to code execution or denial of service.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16234	In PLC WinProladder Version 3.28 and prior, a stack-based buffer overflow vulnerability can be exploited when a valid user opens a specially crafted file, which may allow an attacker to remotely execute arbitrary code.	7.8	More Details
CVE-2020-12302	Improper permissions in the Intel(R) Driver & Support Assistant before version 20.7.26.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2020-5632	InfoCage SiteShell series (Host type SiteShell for IIS V1.4, V1.5, and V1.6, Host type SiteShell for IIS prior to revision V2.0.0.6, V2.1.0.7, V2.1.1.6, V3.0.0.11, V4.0.0.6, V4.1.0.5, and V4.2.0.1, Host type SiteShell for Apache Windows V1.4, V1.5, and V1.6, and Host type SiteShell for Apache Windows prior to revision V2.0.0.6, V2.1.0.7, V2.1.1.6, V3.0.0.11, V4.0.0.6, V4.1.0.5, and V4.2.0.1) allow authenticated attackers to bypass access restriction and to execute arbitrary code with an elevated privilege via a specially crafted executable files.	7.8	More Details
CVE-2020-6654	A DLL Hijacking vulnerability in Eaton's 9000x Programming and Configuration Software v 2.0.38 and prior allows an attacker to execute arbitrary code by replacing the required DLLs with malicious DLLs when the software try to load vci11un6.DLL and cinpl.DLL.	7.8	More Details
CVE-2020-26538	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. It allows attackers to execute arbitrary code via a Trojan horse taskkill.exe in the current working directory.	7.8	More Details
CVE-2020-14375	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. Virtio ring descriptors, and the data they describe are in a region of memory accessible by from both the virtual machine and the host. An attacker in a VM can change the contents of the memory after vhost_crypto has validated it. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-24620	Unisys Stealth(core) before 4.0.134 stores passwords in a recoverable format. Therefore, a search of Enterprise Manager can potentially reveal credentials.	7.8	More Details
CVE-2020-24807	The socket.io-file package through 2.0.31 for Node.js relies on client-side validation of file types, which allows remote attackers to execute arbitrary code by uploading an executable file via a modified JSON name field. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8781	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process.	7.8	More Details
CVE-2020-5987	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin in which guest-supplied parameters remain writable by the guest after the plugin has validated them, which may lead to the guest being able to pass invalid parameters to plugin handlers, which may lead to denial of service or escalation of privileges. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	7.8	More Details
CVE-2020-25776	Trend Micro Antivirus for Mac 2020 (Consumer) is vulnerable to a symbolic link privilege escalation attack where an attacker could exploit a critical file on the system to escalate their privileges. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2020-5981	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, which may lead to denial of service or code execution.	7.8	More Details
CVE-2020-17382	The MSI AmbientLink MsIo64 driver 1.0.0.8 has a Buffer Overflow (0x80102040, 0x80102044, 0x80102050,and 0x80102054).	7.8	More Details
CVE-2020-5984	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin in which it may have the use-after-free vulnerability while freeing some resources, which may lead to denial of service, code execution, and information disclosure. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	7.8	More Details
CVE-2020-21527	There is an Arbitrary file deletion vulnerability in halo v1.1.3. A backup function in the background allows a user, when deleting their backup files, to delete any files on the system through directory traversal.	7.7	More Details
CVE-2020-13323	A vulnerability was discovered in GitLab versions prior 13.1. Under certain conditions private merge requests could be read via Todos	7.7	More Details
CVE-2020-24216	An issue was discovered in the box application on HiSilicon based IPTV/H.264/H.265 video encoders. When the administrator configures a secret URL for RTSP streaming, the stream is still available via its default name such as /0. Unauthenticated attackers can view video streams that are meant to be private.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15598	Trustwave ModSecurity 3.x through 3.0.4 allows denial of service via a special request. NOTE: The discoverer reports "Trustwave has signaled they are disputing our claims." The CVE suggests that there is a security issue with how ModSecurity handles regular expressions that can result in a Denial of Service condition. The vendor does not consider this as a security issue because1) there is no default configuration issue here. An attacker would need to know that a rule using a potentially problematic regular expression was in place, 2) the attacker would need to know the basic nature of the regular expression itself to exploit any resource issues. It's well known that regular expression usage can be taxing on system resources regardless of the use case. It is up to the administrator to decide on when it is appropriate to trade resources for potential security benefit	7.5	More Details
CVE-2019-4326	"HCL AppScan Enterprise security rules update administration section of the web application console is missing HTTP Strict-Transport-Security Header."	7.5	More Details
CVE-2020-25018	Envoy master between 2d69e30 and 3b5acb2 may fail to parse request URL that requires host canonicalization.	7.5	More Details
CVE-2020-25987	MonoCMS Blog 1.0 stores hard-coded admin hashes in the log.xml file in the source files for MonoCMS Blog. Hash type is bcrypt and hashcat mode 3200 can be used to crack the hash.	7.5	More Details
CVE-2020-25613	An issue was discovered in Ruby through 2.5.8, 2.6.x through 2.6.6, and 2.7.x through 2.7.1. WEBrick, a simple HTTP server bundled with Ruby, had not checked the transfer-encoding header value rigorously. An attacker may potentially exploit this issue to bypass a reverse proxy (which also has a poor header check), which may lead to an HTTP Request Smuggling attack.	7.5	More Details
CVE-2020-8782	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution.	7.5	More Details
CVE-2020-25623	Erlang/OTP 22.3.x before 22.3.4.6 and 23.x before 23.1 allows Directory Traversal. An attacker can send a crafted HTTP request to read arbitrary files, if httpd in the inets application is used.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26061	ClickStudios Passwordstate Password Reset Portal prior to build 8501 is affected by an authentication bypass vulnerability. The ResetPassword function does not validate whether the user has successfully authenticated using security questions. An unauthenticated, remote attacker can send a crafted HTTP request to the /account/ResetPassword page to set a new password for any registered user.	7.5	More Details
CVE-2020-14293	conf_datetime in Secudos DOMOS 5.8 allows remote attackers to execute arbitrary commands as root via shell metacharacters in the zone field (obtained from the web interface).	7.5	More Details
CVE-2020-25644	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2020-11979	As mitigation for CVE-2020-1945 Apache Ant 1.10.8 changed the permissions of temporary files it created so that only the current user was allowed to access them. Unfortunately the fixcrlf task deleted the temporary file and created a new one without said protection, effectively nullifying the effort. This would still allow an attacker to inject modified source files into the build process.	7.5	More Details
CVE-2020-25866	In Wireshark 3.2.0 to 3.2.6 and 3.0.0 to 3.0.13, the BLIP protocol dissector has a NULL pointer dereference because a buffer was sized for compressed (not uncompressed) messages. This was addressed in epan/dissectors/packet-blip.c by allowing reasonable compression ratios and rejecting ZIP bombs.	7.5	More Details
CVE-2020-25862	In Wireshark 3.2.0 to 3.2.6, 3.0.0 to 3.0.13, and 2.6.0 to 2.6.20, the TCP dissector could crash. This was addressed in epan/dissectors/packet-tcp.c by changing the handling of the invalid 0xFFFF checksum.	7.5	More Details
CVE-2020-7466	The PPP implementation of MPD before 5.9 allows a remote attacker who can send specifically crafted PPP authentication message to cause the daemon to read beyond allocated memory buffer, which would result in a denial of service condition.	7.5	More Details
CVE-2020-9486	In Apache NiFi 1.10.0 to 1.11.4, the NiFi stateless execution engine produced log output which included sensitive property values. When a flow was triggered, the flow definition configuration JSON was printed, potentially containing sensitive values in plaintext.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9487	In Apache NiFi 1.0.0 to 1.11.4, the NiFi download token (one-time password) mechanism used a fixed cache size and did not authenticate a request to create a download token, only when attempting to use the token to access the content. An unauthenticated user could repeatedly request download tokens, preventing legitimate users from requesting download tokens.	7.5	More Details
CVE-2020-9491	In Apache NiFi 1.2.0 to 1.11.4, the NiFi UI and API were protected by mandating TLS v1.2, as well as listening connections established by processors like ListenHTTP, HandleHttpRequest, etc. However intracluster communication such as cluster request replication, Site-to-Site, and load balanced queues continued to support TLS v1.0 or v1.1.	7.5	More Details
CVE-2020-26511	The wpo365-login plugin before v11.7 for WordPress allows use of a symmetric algorithm to decrypt a JWT token. This leads to authentication bypass.	7.5	More Details
CVE-2020-24697	An issue was discovered in PowerDNS Authoritative through 4.3.0 when --enable-experimental-gss-tsig is used. A remote, unauthenticated attacker can cause a denial of service by sending crafted queries with a GSS-TSIG signature.	7.5	More Details
CVE-2020-25863	In Wireshark 3.2.0 to 3.2.6, 3.0.0 to 3.0.13, and 2.6.0 to 2.6.20, the MIME Multipart dissector could crash. This was addressed in epan/dissectors/packet-multipart.c by correcting the deallocation of invalid MIME parts.	7.5	More Details
CVE-2020-26575	In Wireshark through 3.2.7, the Facebook Zero Protocol (aka FBZERO) dissector could enter an infinite loop. This was addressed in epan/dissectors/packet-fbzero.c by correcting the implementation of offset advancement.	7.5	More Details
CVE-2017-18924	oauth2-server (aka node-oauth2-server) through 3.1.1 implements OAuth 2.0 without PKCE. It does not prevent authorization code injection. This is similar to CVE-2020-7692. NOTE: the vendor states 'As RFC7636 is an extension, I think the claim in the Readme of "RFC 6749 compliant" is valid and not misleading and I also therefore wouldn't describe this as a "vulnerability" with the library per se.	7.5	More Details
CVE-2020-26540	An issue was discovered in Foxit Reader and PhantomPDF before 4.1 on macOS. Because the Hardened Runtime protection mechanism is not applied to code signing, code injection (or an information leak) can occur.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12127	An information disclosure vulnerability in the /cgi-bin/ExportAllSettings.sh endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to leak router settings, including cleartext login details, DNS settings, and other sensitive information without authentication.	7.5	More Details
CVE-2020-24219	An issue was discovered on URayTech IPTV/H.264/H.265 video encoders through 1.97. Attackers can send crafted unauthenticated HTTP requests to exploit path traversal and pattern-matching programming flaws, and retrieve any file from the device's file system, including the configuration file with the cleartext administrative password.	7.5	More Details
CVE-2020-21525	Halo V1.1.3 is affected by: Arbitrary File reading. In an interface that reads files in halo v1.1.3, a directory traversal check is performed on the input path parameter, but the startsWith function can be used to bypass it.	7.5	More Details
CVE-2020-26597	An issue was discovered on LG mobile devices with Android OS 9.0 and 10 software. The Wi-Fi subsystem has incorrect input validation, leading to a crash. The LG ID is LVE-SMP-200022 (October 2020).	7.5	More Details
CVE-2020-26602	An issue was discovered in EthernetNetwork on Samsung mobile devices with O(8.1), P(9.0), Q(10.0), and R(11.0) software. PendingIntent allows sdcard access by an unprivileged process. The Samsung ID is SVE-2020-18392 (October 2020).	7.5	More Details
CVE-2020-26149	NATS nats.js before 2.0.0-209, nats.ws before 1.0.0-111, and nats.deno before 1.0.0-9 allow credential disclosure from a client to a server.	7.5	More Details
CVE-2020-26600	An issue was discovered on Samsung mobile devices with Q(10.0) software. Auto Hotspot allows attackers to obtain sensitive information. The Samsung ID is SVE-2020-17288 (October 2020).	7.5	More Details
CVE-2020-26148	md_push_block_bytes in md4c.c in md4c 0.4.5 allows attackers to trigger use of uninitialized memory, and cause a denial of service (e.g., assertion failure) via a malformed Markdown document.	7.5	More Details
CVE-2020-15488	Re:Desk 2.3 allows insecure file upload.	7.5	More Details
CVE-2020-26160	jwt-go before 4.0.0-preview1 allows attackers to bypass intended access restrictions in situations with []string{} for m["aud"] (which is allowed by the specification). Because the type assertion fails, "" is the value of aud. This is a security problem if the JWT token is presented to a service that lacks its own audience check.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13951	Attackers can use public NetTest web service of Apache OpenMeetings 4.0.0-5.0.0 to organize denial of service attack.	7.5	More Details
CVE-2020-26598	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, and 9.0 software. The Network Management component could allow an unauthorized actor to kill a TCP connection. The LG ID is LVE-SMP-200023 (October 2020).	7.5	More Details
CVE-2020-1902	A user running a quick search on a highly forwarded message on WhatsApp for Android from v2.20.108 to v2.20.140 or WhatsApp Business for Android from v2.20.35 to v2.20.49 could have been sent to the Google service over plain HTTP.	7.5	More Details
CVE-2020-26604	An issue was discovered in SystemUI on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. PendingIntent allows an unprivileged process to access contact numbers. The Samsung ID is SVE-2020-18467 (October 2020).	7.5	More Details
CVE-2020-26601	An issue was discovered in DirEncryptService on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. PendingIntent with an empty intent is mishandled, allowing an attacker to perform a privileged action via a modified intent. The Samsung ID is SVE-2020-18034 (October 2020).	7.5	More Details
CVE-2020-15174	In Electron before versions 11.0.0-beta.1, 10.0.1, 9.3.0 or 8.5.1 the `will-navigate` event that apps use to prevent navigations to unexpected destinations as per our security recommendations can be bypassed when a sub-frame performs a top-frame navigation across sites. The issue is patched in versions 11.0.0-beta.1, 10.0.1, 9.3.0 or 8.5.1 As a workaround sandbox all your iframes using the sandbox attribute. This will prevent them creating top-frame navigations and is good practice anyway.	7.5	More Details
CVE-2019-20902	Upgrading Crowd via XML Data Transfer can reactivate a disabled user from OpenLDAP. The affected versions are from before version 3.4.6 and from 3.5.0 before 3.5.1.	7.5	More Details
CVE-2019-20922	Handlebars before 4.4.5 allows Regular Expression Denial of Service (ReDoS) because of eager matching. The parser may be forced into an endless loop while processing crafted templates. This may allow attackers to exhaust system resources.	7.5	More Details
CVE-2020-13343	An issue has been discovered in GitLab affecting all versions starting from 11.2. Unauthorized Users Can View Custom Project Template	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-11765	In Apache Hadoop versions 3.0.0-alpha2 to 3.0.0, 2.9.0 to 2.9.2, 2.8.0 to 2.8.5, any users can access some servlets without authentication when Kerberos authentication is enabled and SPNEGO through HTTP is not enabled.	7.5	More Details
CVE-2020-26605	An issue was discovered on Samsung mobile devices with Q(10.0) and R(11.0) (Exynos chipsets) software. They allow attackers to obtain sensitive information by reading a log. The Samsung ID is SVE-2020-18596 (October 2020).	7.5	More Details
CVE-2020-26606	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. An attacker can access certain Secure Folder content via a debugging command. The Samsung ID is SVE-2020-18673 (October 2020).	7.5	More Details
CVE-2020-4576	IBM WebSphere Application Server 7.5, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 184428.	7.5	More Details
CVE-2020-26150	info.php in Logaritmo Aware CallManager 2012 allows remote attackers to obtain sensitive information via a direct request, which calls the phpinfo function.	7.5	More Details
CVE-2019-19199	REDDOXX MailDepot 2032 SP2 2.2.1242 has Insufficient Session Expiration because tokens are not invalidated upon a logout.	7.4	More Details
CVE-2020-7736	The package bmoor before 0.8.12 are vulnerable to Prototype Pollution via the set function.	7.3	More Details
CVE-2020-7737	All versions of package safetydance are vulnerable to Prototype Pollution via the set function.	7.3	More Details
CVE-2020-8243	A vulnerability in the Pulse Connect Secure < 9.1R8.2 admin web interface could allow an authenticated attacker to upload custom template to perform an arbitrary code execution.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15849	Re:Desk 2.3 has a blind authenticated SQL injection vulnerability in the SettingsController class, in the actionEmailTemplates() method. A malicious actor with access to an administrative account could abuse this vulnerability to recover sensitive data from the application's database, allowing for authorization bypass and taking over additional accounts by means of modifying password-reset tokens stored in the database. Remote command execution is also possible by leveraging this to abuse the Yii framework's bizRule functionality, allowing for arbitrary PHP code to be executed by the application. Remote command execution is also possible by using this together with a separate insecure file upload vulnerability (CVE-2020-15488).	7.2	More Details
CVE-2020-18184	In PluxXml V5.7,the theme edit function /PluXml/core/admin/parametres_edittpl.php allows remote attackers to execute arbitrary PHP code by placing this code into a template.	7.2	More Details
CVE-2020-13322	A vulnerability was discovered in GitLab versions after 12.9. Due to improper verification of permissions, an unauthorized user can create and delete deploy tokens.	7.2	More Details
CVE-2020-13337	An issue has been discovered in GitLab affecting versions from 12.10 to 12.10.12 that allowed for a stored XSS payload to be added as a group name.	7.2	More Details
CVE-2020-24397	An issue was discovered in the client side of Zoho ManageEngine Desktop Central 10.0.0.SP-534. An attacker-controlled server can trigger an integer overflow in InternetSendRequestEx and InternetSendRequestByBitrate that leads to a heap-based buffer overflow and Remote Code Execution with SYSTEM privileges.	7.2	More Details
CVE-2020-14030	An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. It stores SMS messages in .NET serialized format on the filesystem. By generating (and writing to the disk) malicious .NET serialized files, an attacker can trick the product into deserializing them, resulting in arbitrary code execution.	7.2	More Details
CVE-2020-25643	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5988	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which allocated memory can be freed twice, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	7.1	More Details
CVE-2020-13325	A vulnerability was discovered in GitLab versions prior 13.1. The comment section of the issue page was not restricting the characters properly, potentially resulting in a denial of service.	7.1	More Details
CVE-2020-14377	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. A complete lack of validation of attacker-controlled parameters can lead to a buffer over read. The results of the over read are then written back to the guest virtual machine memory. This vulnerability can be used by an attacker in a virtual machine to read significant amounts of host memory. The highest threat from this vulnerability is to data confidentiality and system availability.	7.1	More Details
CVE-2020-5985	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which an input data length is not validated, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	7.1	More Details
CVE-2020-5983	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin and the host driver kernel module, in which the potential exists to write to a memory location that is outside the intended boundary of the frame buffer memory allocated to guest operating systems, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	7.1	More Details
CVE-2020-16844	In Istio 1.5.0 though 1.5.8 and Istio 1.6.0 through 1.6.7, when users specify an AuthorizationPolicy resource with DENY actions using wildcard suffixes (e.g. *-some-suffix) for source principals or namespace fields, callers will never be denied access, bypassing the intended policy.	6.8	More Details
CVE-2020-25816	HashiCorp Vault and Vault Enterprise versions 1.0 and newer allowed leases created with a batch token to outlive their TTL because expiration time was not scheduled correctly. Fixed in 1.4.7 and 1.5.4.	6.8	More Details
CVE-2020-25637	A double free memory issue was found to occur in the libvirt API, in versions before 6.8.0, responsible for requesting information about network interfaces of a running QEMU domain. This flaw affects the polkit access control driver. Specifically, clients connecting to the read-write socket with limited ACL permissions could use this flaw to crash the libvirt daemon, resulting in a denial of service, or potentially escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25636	A flaw was found in Ansible Base when using the aws_ssm connection plugin as there is no namespace separation for file transfers. Files are written directly to the root bucket, making possible to have collisions when running multiple ansible processes. This issue affects mainly the service availability.	6.6	More Details
CVE-2020-13329	An issue has been discovered in GitLab affecting versions from 12.6.2 prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the blob view feature.	6.5	More Details
CVE-2020-26541	The Linux kernel through 5.8.13 does not properly enforce the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. This affects certs/blacklist.c and certs/system_keyring.c.	6.5	More Details
CVE-2020-15664	By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, Firefox ESR < 78.2, and Firefox for Android < 80.	6.5	More Details
CVE-2020-5422	BOSH System Metrics Server releases prior to 0.1.0 exposed the UAA password as a flag to a process running on the BOSH director. It exposed the password to any user or process with access to the same VM (through ps or looking at process details).	6.5	More Details
CVE-2020-25986	A Cross Site Request Forgery (CSRF) vulnerability in MonoCMS Blog 1.0 allows attackers to change the password of a user.	6.5	More Details
CVE-2020-15666	When trying to load a non-video in an audio/video context the exact status code (200, 302, 404, 500, 412, 403, etc.) was disclosed via the MediaError Message. This level of information leakage is inconsistent with the standardized onerror/onsuccess disclosure and can lead to inferring login status to services or device discovery on a local network among other attacks. This vulnerability affects Firefox < 80 and Firefox for Android < 80.	6.5	More Details
CVE-2020-24568	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.1. There is a blind SQL injection in the lancompenent component, allowing logged-in attackers to discover arbitrary information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8223	A logic error in Nextcloud Server 19.0.0 caused a privilege escalation allowing malicious users to reshare with higher permissions than they got assigned themselves.	6.5	More Details
CVE-2020-13296	An issue has been discovered in GitLab affecting versions >=10.7 <13.0.14, >=13.1.0 <13.1.8, >=13.2.0 <13.2.6. Improper Access Control for Deploy Tokens	6.5	More Details
CVE-2020-24570	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.1. There is a CSRF issue (with resultant SSRF) in the com_mb24proxy module, allowing attackers to steal session information from logged-in users with a crafted link.	6.5	More Details
CVE-2020-5788	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to delete arbitrary files on disk via the admin/system/admin/certificates/delete action.	6.5	More Details
CVE-2020-13320	An issue has been discovered in GitLab before version 12.10.13 that allowed a project member with limited permissions to view the project security dashboard.	6.5	More Details
CVE-2020-26137	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.	6.5	More Details
CVE-2020-13324	A vulnerability was discovered in GitLab versions prior to 13.1. Under certain conditions the private activity of a user could be exposed via the API.	6.5	More Details
CVE-2020-5784	Server-Side Request Forgery in Teltonika firmware TRB2_R_00.02.04.3 allows a low privileged user to cause the application to perform HTTP GET requests to arbitrary URLs.	6.5	More Details
CVE-2020-5787	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to delete arbitrary files on disk via the admin/services/packages/remove action.	6.5	More Details
CVE-2020-5789	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to read the contents of arbitrary files on disk.	6.5	More Details
CVE-2020-24356	`cloudflared` versions prior to 2020.8.1 contain a local privilege escalation vulnerability on Windows systems. When run on a Windows system, `cloudflared` searches for configuration files which could be abused by a malicious entity to execute commands as a privileged user. Version 2020.8.1 fixes this issue.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19393	The Web application on Rittal CMC PU III 7030.000 V3.00 V3.11.00_2 to V3.15.70_4 devices fails to sanitize user input on the system configurations page. This allows an attacker to backdoor the device with HTML and browser-interpreted content (such as JavaScript or other client-side scripts) as the content is always displayed after and before login. Persistent XSS allows an attacker to modify displayed content or to change the victim's information. Successful exploitation requires access to the web management interface, either with valid credentials or a hijacked session.	6.1	More Details
CVE-2020-13168	SysAid 20.1.11b26 allows reflected XSS via the ForgotPassword.jsp accountid parameter.	6.1	More Details
CVE-2020-23832	A Persistent Cross-Site Scripting (XSS) vulnerability in message_admin.php in Projectworlds Car Rental Management System v1.0 allows unauthenticated remote attackers to harvest an admin login session cookie and steal an admin session upon an admin login.	6.1	More Details
CVE-2020-5631	Stored cross-site scripting vulnerability in CMONOS.JP ver2.0.20191009 and earlier allows remote attackers to inject arbitrary script via unspecified vectors.	6.1	More Details
CVE-2019-20921	bootstrap-select before 1.13.6 allows Cross-Site Scripting (XSS). It does not escape title values in OPTION elements. This may allow attackers to execute arbitrary JavaScript in a victim's browser.	6.1	More Details
CVE-2019-4725	IBM Security Access Manager Appliance 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 172131.	6.1	More Details
CVE-2020-15677	By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect) rather than the site the file was actually downloaded from. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.	6.1	More Details
CVE-2020-14223	HCL Digital Experience 8.5, 9.0, 9.5 is susceptible to cross-site scripting (XSS). The vulnerability could be employed in a reflected or non-persistent XSS attack.	6.1	More Details
CVE-2020-5785	Insufficient output sanitization in Teltonika firmware TRB2_R_00.02.04.3 allows an unauthenticated attacker to conduct reflected cross-site scripting via a crafted ‘action’ or ‘pkg_name’ parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25626	A flaw was found in Django REST Framework versions before 3.12.0 and before 3.11.2. When using the browseable API viewer, Django REST Framework fails to properly escape certain strings that can come from user input. This allows a user who can control those strings to inject malicious <script> tags, leading to a cross-site-scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-26523	Froala Editor before 3.2.2 allows XSS via pasted content.	6.1	More Details
CVE-2020-15234	ORY Fosite is a security first OAuth2 & OpenID Connect framework for Go. In Fosite before version 0.34.1, the OAuth 2.0 Client's registered redirect URLs and the redirect URL provided at the OAuth2 Authorization Endpoint where compared using strings.ToLower while they should have been compared with a simple string match. This allows an attacker to register a client with allowed redirect URL https://example.com/callback. Then perform an OAuth2 flow and requesting redirect URL https://example.com/CALLBACK. Instead of an error (invalid redirect URL), the browser is redirected to https://example.com/CALLBACK with a potentially successful OAuth2 response, depending on the state of the overall OAuth2 flow (the user might still deny the request for example). This vulnerability has been patched in ORY Fosite v0.34.1.	6.1	More Details
CVE-2020-15233	ORY Fosite is a security first OAuth2 & OpenID Connect framework for Go. In Fosite from version 0.30.2 and before version 0.34.1, there is an issue in which an an attacker can override the registered redirect URL by performing an OAuth flow and requesting a redirect URL that is to the loopback adapter. Attackers can provide both custom URL query parameters to their loopback redirect URL, as well as actually overriding the host of the registered redirect URL. These attacks are only applicable in scenarios where the attacker has access over the loopback interface. This vulnerability has been patched in ORY Fosite v0.34.1.	6.1	More Details
CVE-2020-8238	A vulnerability in the authenticated user web interface of Pulse Connect Secure and Pulse Policy Secure < 9.1R8.2 could allow attackers to conduct Cross-Site Scripting (XSS).	6.1	More Details
CVE-2020-15676	Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22481	An issue was discovered in HFish 0.5.1. When a payload is inserted where the password is entered, XSS code is triggered when the administrator views the information.	6.1	More Details
CVE-2020-14294	An issue was discovered in Secudos Qiata FTA 1.70.19. The comment feature allows persistent XSS that is executed when reading transfer comments or the global notice board.	6.1	More Details
CVE-2020-26043	An issue was discovered in Hoosk CMS v1.8.0. There is a XSS vulnerability in install/index.php	6.1	More Details
CVE-2020-25761	Projectworlds Visitor Management System in PHP 1.0 allows XSS. The file myform.php does not perform input validation on the request parameters. An attacker can inject javascript payloads in the parameters to perform various attacks such as stealing of cookies,sensitive information etc.	6.1	More Details
CVE-2020-26134	Live Helper Chat before 3.44v allows stored XSS in chat messages with an operator via BBCode.	6.1	More Details
CVE-2020-26135	Live Helper Chat before 3.44v allows reflected XSS via the setsettingajax PATH_INFO.	6.1	More Details
CVE-2020-7709	This affects the package json-pointer before 0.6.1. Multiple reference of object using slash is supported.	6.0	More Details
CVE-2020-15237	In Shrine before version 3.3.0, when using the `derivation_endpoint` plugin, it's possible for the attacker to use a timing attack to guess the signature of the derivation URL. The problem has been fixed by comparing sent and calculated signature in constant time, using `Rack::Utils.secure_compare`. Users using the `derivation_endpoint` plugin are urged to upgrade to Shrine 3.3.0 or greater. A possible workaround is provided in the linked advisory.	5.9	More Details
CVE-2020-15235	In RACTF before commit f3dc89b, unauthenticated users are able to get the value of sensitive config keys that would normally be hidden to everyone except admins. All versions after commit f3dc89b9f6ab1544a289b3efc06699b13d63e0bd(3/10/20) are patched.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8109	A vulnerability has been discovered in the ace.xmd parser that results from a lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. This can result in denial-of-service. This issue affects: Bitdefender Engines version 7.84892 and prior versions.	5.9	More Details
CVE-2020-8110	A vulnerability has been discovered in the ceva_emu.cvd module that results from a lack of proper validation of user-supplied data, which can result in a pointer that is fetched from uninitialized memory. This can lead to denial-of-service. This issue affects: Bitdefender Engines version 7.84897 and prior versions.	5.9	More Details
CVE-2020-24721	An issue was discovered in the GAEN (aka Google/Apple Exposure Notifications) protocol through 2020-09-29, as used in COVID-19 applications on Android and iOS. It allows a user to be put in a position where he or she can be coerced into proving or disproving an exposure notification, because of the persistent state of a private framework.	5.7	More Details
CVE-2019-14558	Insufficient control flow management in BIOS firmware for 8th, 9th, 10th Generation Intel(R) Core(TM), Intel(R) Celeron(R) Processor 4000 & 5000 Series Processors may allow an authenticated user to potentially enable denial of service via adjacent access.	5.7	More Details
CVE-2020-15215	Electron before versions 11.0.0-beta.6, 10.1.2, 9.3.1 or 8.5.2 is vulnerable to a context isolation bypass. Apps using both `contextIsolation` and `sandbox: true` are affected. Apps using both `contextIsolation` and `nodeIntegrationInSubFrames: true` are affected. This is a context isolation bypass, meaning that code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions.	5.6	More Details
CVE-2020-25641	A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	5.5	More Details
CVE-2020-1903	An issue when unzipping docx, pptx, and xlsx documents in WhatsApp for iOS prior to v2.20.61 and WhatsApp Business for iOS prior to v2.20.61 could have resulted in an out-of-memory denial of service. This issue would have required the receiver to explicitly open the attachment if it was received from a number not in the receiver's WhatsApp contacts.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8671	Insufficient control flow management in BIOS firmware 8th, 9th Generation Intel(R) Core(TM) Processors and Intel(R) Celeron(R) Processor 4000 Series may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-13345	An issue has been discovered in GitLab affecting all versions starting from 10.8. Reflected XSS on Multiple Routes	5.5	More Details
CVE-2020-26570	The Oberthur smart card software driver in OpenSC before 0.21.0-rc1 has a heap-based buffer overflow in sc_oberthur_read_file.	5.5	More Details
CVE-2020-13940	In Apache NiFi 1.0.0 to 1.11.4, the notification service manager and various policy authorizer and user group provider objects allowed trusted administrators to inadvertently configure a potentially malicious XML file. The XML file has the ability to make external calls to services (via XXE).	5.5	More Details
CVE-2020-26571	The gemsafe GPK smart card software driver in OpenSC before 0.21.0-rc1 has a stack-based buffer overflow in sc_pkcs15emu_gemsafeGPK_init.	5.5	More Details
CVE-2020-0571	Improper conditions check in BIOS firmware for 8th Generation Intel(R) Core(TM) Processors and Intel(R) Pentium(R) Silver Processor Series may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2020-26572	The TCOS smart card software driver in OpenSC before 0.21.0-rc1 has a stack-based buffer overflow in tcos_decipher.	5.5	More Details
CVE-2020-4528	IBM MQ Appliance (IBM DataPower Gateway 10.0.0.0 and 2018.4.1.0 through 2018.4.1.12) could allow a local user, under special conditions, to obtain highly sensitive information from log files. IBM X-Force ID: 182658.	5.5	More Details
CVE-2020-5989	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which it can dereference a NULL pointer, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	5.5	More Details
CVE-2020-1904	A path validation issue in WhatsApp for iOS prior to v2.20.61 and WhatsApp Business for iOS prior to v2.20.61 could have allowed for directory traversal overwriting files when sending specially crafted docx, xlsx, and pptx files as attachments to messages.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5986	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which an input data size is not validated, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	5.5	More Details
CVE-2020-26519	Artifex MuPDF before 1.18.0 has a heap based buffer over-write when parsing JBIG2 files allowing attackers to cause a denial of service.	5.5	More Details
CVE-2020-26536	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. There is a NULL pointer dereference via a crafted PDF document.	5.5	More Details
CVE-2019-18991	A partial authentication bypass vulnerability exists on Atheros AR9132 3.60(AMX.8), AR9283 1.85, and AR9285 1.0.0.12NA devices. The vulnerability allows sending an unencrypted data frame to a WPA2-protected WLAN router where the packet is routed through the network. If successful, a response is sent back as an encrypted frame, which would allow an attacker to discern information or potentially modify data.	5.4	More Details
CVE-2019-18990	A partial authentication bypass vulnerability exists on Realtek RTL8812AR 1.21WW, RTL8196D 1.0.0, RTL8192ER 2.10, and RTL8881AN 1.09 devices. The vulnerability allows sending an unencrypted data frame to a WPA2-protected WLAN router where the packet is routed through the network. If successful, a response is sent back as an encrypted frame, which would allow an attacker to discern information or potentially modify data.	5.4	More Details
CVE-2019-18989	A partial authentication bypass vulnerability exists on Mediatek MT7620N 1.06 devices. The vulnerability allows sending an unencrypted data frame to a WPA2-protected WLAN router where the packet is routed through the network. If successful, a response is sent back as an encrypted frame, which would allow an attacker to discern information or potentially modify data.	5.4	More Details
CVE-2020-24860	CMS Made Simple 2.2.14 allows an authenticated user with access to the Content Manager to edit content and put persistent XSS payload in the affected text fields. The user can get cookies from every authenticated user who visits the website.	5.4	More Details
CVE-2020-24861	GetSimple CMS 3.3.16 allows in parameter 'permalink' on the Settings page persistent Cross Site Scripting which is executed when you create and open a new page	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13338	An issue has been discovered in GitLab affecting versions prior to 12.10.13, 13.0.8, 13.1.2. A stored cross-site scripting vulnerability was discovered when editing references.	5.4	More Details
CVE-2020-26166	The file upload functionality in qdPM 9.1 doesn't check the file description, which allows remote authenticated attackers to inject web script or HTML via the attachments info parameter, aka XSS. This can occur during creation of a ticket, project, or task.	5.4	More Details
CVE-2019-20903	The hyperlinks functionality in atlaskit/editor-core in before version 113.1.5 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in link targets.	5.4	More Details
CVE-2020-24627	A remote stored xss vulnerability was discovered in HPE KVM IP Console Switches version(s): G2 4x1Ex32 Prior to 2.8.3.	5.4	More Details
CVE-2020-12869	RainbowFish PacsOne Server 6.8.4 allows XSS.	5.4	More Details
CVE-2020-7069	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.	5.4	More Details
CVE-2020-22842	CMS Made Simple before 2.2.15 allows XSS via the m1_mod parameter in a ModuleManager local_uninstall action to admin/moduleinterface.php.	5.4	More Details
CVE-2020-13331	An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the Wiki pasges.	5.4	More Details
CVE-2020-26603	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Sticker Center allows directory traversal for an unprivileged process to read arbitrary files. The Samsung ID is SVE-2020-18433 (October 2020).	5.3	More Details
CVE-2020-26599	An issue was discovered on Samsung mobile devices with Q(10.0) software. The DynamicLockscreen Terms and Conditions can be accepted without authentication. The Samsung ID is SVE-2020-17079 (October 2020).	5.3	More Details
CVE-2019-4325	"HCL AppScan Enterprise makes use of broken or risky cryptographic algorithm to store REST API user details."	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1901	Receiving a large text message containing URLs in WhatsApp for iOS prior to v2.20.91.4 could have caused the application to freeze while processing the message.	5.3	More Details
CVE-2020-5132	SonicWall SSL-VPN products and SonicWall firewall SSL-VPN feature misconfiguration leads to possible DNS flaw known as domain name collision vulnerability. When the users publicly display their organization's internal domain names in the SSL-VPN authentication page, an attacker with knowledge of internal domain names can potentially take advantage of this vulnerability.	5.3	More Details
CVE-2020-13953	In Apache Tapestry from 5.4.0 to 5.5.0, crafting specific URLs, an attacker can download files inside the WEB-INF folder of the WAR being run.	5.3	More Details
CVE-2020-8228	A missing rate limit in the Preferred Providers app 1.7.0 allowed an attacker to set the password an uncontrolled amount of times.	5.3	More Details
CVE-2020-25200	Pritunl 1.29.2145.25 allows attackers to enumerate valid VPN usernames via a series of /auth/session login attempts. Initially, the server will return error 401. However, if the username is valid, then after 20 login attempts, the server will start responding with error 400. Invalid usernames will receive error 401 indefinitely. Note: This has been disputed by the vendor as not a vulnerability. They argue that this is an intended design	5.3	More Details
CVE-2020-26526	An issue was discovered in Damstra Smart Asset 2020.7. It is possible to enumerate valid usernames on the login page. The application sends a different server response when the username is invalid than when the username is valid ("Unable to find an APIDomain" versus "Wrong email or password").	5.3	More Details
CVE-2020-19676	Nacos 1.1.4 is affected by: Incorrect Access Control. An environment can be set up locally to get the service details interface. Then other Nacos service names can be accessed through the service list interface. Service details can then be accessed when not logged in. (detail:https://github.com/alibaba/nacos/issues/2284)	5.3	More Details
CVE-2020-26524	CodeLathe FileCloud before 20.2.0.11915 allows username enumeration.	5.3	More Details
CVE-2020-25635	A flaw was found in Ansible Base when using the aws_ssm connection plugin as garbage collector is not happening after playbook run is completed. Files would remain in the bucket exposing the data. This issue affects directly data confidentiality.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8256	A vulnerability in the Pulse Connect Secure < 9.1R8.2 admin web interface could allow an authenticated attacker to gain arbitrary file reading access through Pulse Collaboration via XML External Entity (XXE) vulnerability.	4.9	More Details
CVE-2020-21244	An issue was discovered in FrontAccounting 2.4.7. There is a Directory Traversal vulnerability that can empty folder via admin/inst_lang.php.	4.9	More Details
CVE-2020-19670	In Niushop B2B2C Multi-Business Basic Edition V1.11, authentication can be bypassed, causing administrators to reset any passwords.	4.9	More Details
CVE-2020-25288	An issue was discovered in MantisBT before 2.24.3. When editing an Issue in a Project where a Custom Field with a crafted Regular Expression property is used, improper escaping of the corresponding form input's pattern attribute allows HTML injection and, if CSP settings permit, execution of arbitrary JavaScript.	4.8	More Details
CVE-2020-13328	An issue has been discovered in GitLab affecting versions prior to 13.1.2, 13.0.8 and 12.10.13. GitLab was vulnerable to a stored XSS by using the PyPi files API.	4.8	More Details
CVE-2020-25830	An issue was discovered in MantisBT before 2.24.3. Improper escaping of a custom field's name allows an attacker to inject HTML and, if CSP settings permit, achieve execution of arbitrary JavaScript when attempting to update said custom field via bug_actiongroup_page.php.	4.8	More Details
CVE-2020-13330	An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS in import the Bitbucket project feature.	4.4	More Details
CVE-2020-5982	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) scheduler, in which the software does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests, which may lead to denial of service.	4.4	More Details
CVE-2019-14556	Improper initialization in BIOS firmware for 8th, 9th, 10th Generation Intel(R) Core(TM), Intel(R) Celeron(R) Processor 4000 & 5000 Series Processors may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2020-13794	Harbor 1.9.* 1.10.* and 2.0.* allows Exposure of Sensitive Information to an Unauthorized Actor.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15594	An SSRF issue was discovered in Zoho Application Control Plus before version 10.0.511. The mail gateway configuration feature allows an attacker to perform a scan in order to discover open ports on a machine as well as available machines on the network segment on which the instance of the product is deployed.	4.3	More Details
CVE-2020-15595	An issue was discovered in Zoho Application Control Plus before version 10.0.511. The Element Configuration feature (to configure elements included in the scope of elements managed by the product) allows an attacker to retrieve the entire list of the IP ranges and subnets configured in the product and consequently obtain information about the cartography of the internal networks to which the product has access.	4.3	More Details
CVE-2020-13326	A vulnerability was discovered in GitLab versions prior to 13.1. Under certain conditions the restriction for Github project import could be bypassed.	4.3	More Details
CVE-2020-13333	A potential DOS vulnerability was discovered in GitLab versions 13.1, 13.2 and 13.3. The api to update an asset as a link from a release had a regex check which caused exponential number of backtracks for certain user supplied values resulting in high CPU usage.	4.3	More Details
CVE-2020-24569	An issue was discovered in MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 through 2.6.1. There is a blind SQL injection in the knximport component via an advanced attack vector, allowing logged in attackers to discover arbitrary information.	4.3	More Details
CVE-2020-13319	An issue has been discovered in GitLab affecting versions prior to 13.1.2, 13.0.8 and 12.10.13. Missing permission check for adding time spent on an issue.	4.3	More Details
CVE-2020-8235	Missing access control in Nextcloud Deck 1.0.4 caused an insecure direct object reference allowing an attacker to view all attachments.	4.3	More Details
CVE-2020-25781	An issue was discovered in file_download.php in MantisBT before 2.24.3. Users without access to view private issue notes are able to download the (supposedly private) attachments linked to these notes by accessing the corresponding file download URL directly.	4.3	More Details
CVE-2020-15665	Firefox did not reset the address bar after the beforeunload dialog was shown if the user chose to remain on the page. This could have resulted in an incorrect URL being shown when used in conjunction with other unexpected browser behaviors. This vulnerability affects Firefox < 80.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7070	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.	4.3	More Details
CVE-2020-17482	An issue has been found in PowerDNS Authoritative Server before 4.3.1 where an authorized user with the ability to insert crafted records into a zone might be able to leak the content of uninitialized memory.	4.3	More Details
CVE-2020-15668	A lock was missing when accessing a data structure and importing certificate information into the trust database. This vulnerability affects Firefox < 80 and Firefox for Android < 80.	4.3	More Details
CVE-2020-14183	Affected versions of Jira Server & Data Center allow a remote attacker with limited (non-admin) privileges to view a Jira instance's Support Entitlement Number (SEN) via an Information Disclosure vulnerability in the HTTP Response headers. The affected versions are before version 7.13.18, from version 8.0.0 before 8.5.9, and from version 8.6.0 before 8.12.1.	4.3	More Details
CVE-2020-25803	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via FreeMarker template exposed objects. This issue affects: Crafter Software Crafter CMS 3.0 versions prior to 3.0.27; 3.1 versions prior to 3.1.7.	4.2	More Details
CVE-2020-25802	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via Groovy scripting. This issue affects: Crafter Software Crafter CMS 3.0 versions prior to 3.0.27; 3.1 versions prior to 3.1.7.	4.2	More Details
CVE-2020-13336	An issue has been discovered in GitLab affecting versions from 11.8 before 12.10.13. GitLab was vulnerable to a stored XSS by in the error tracking feature.	4.0	More Details
CVE-2019-17098	Use of hard-coded cryptographic key vulnerability in August Connect Wi-Fi Bridge App, Connect Firmware allows an attacker to decrypt an intercepted payload containing the Wi-Fi network authentication credentials. This issue affects: August Connect Wi-Fi Bridge App version v10.11.0 and prior versions on Android. August Connect Firmware version 2.2.12 and prior versions.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15228	In the `@actions/core` npm module before version 1.2.6,`addPath` and `exportVariable` functions communicate with the Actions Runner over stdout by generating a string in a specific format. Workflows that log untrusted data to stdout may invoke these commands, resulting in the path or environment variables being modified without the intention of the workflow or action author. The runner will release an update that disables the `set-env` and `add-path` workflow commands in the near future. For now, users should upgrade to `@actions/core v1.2.6` or later, and replace any instance of the `set-env` or `add-path` commands in their workflows with the new Environment File Syntax. Workflows and actions using the old commands or older versions of the toolkit will start to warn, then error out during workflow execution.	3.5	More Details
CVE-2020-15239	In xmpp-http-upload before version 0.4.0, when the GET method is attacked, attackers can read files which have a `.data` suffix and which are accompanied by a JSON file with the `.meta` suffix. This can lead to Information Disclosure and in some shared-hosting scenarios also to circumvention of authentication or other limitations on the outbound (GET) traffic. For example, in a scenario where a single server has multiple instances of the application running (with separate DATA_ROOT settings), an attacker who has knowledge about the directory structure is able to read files from any other instance to which the process has read access. If instances have individual authentication (for example, HTTP authentication via a reverse proxy, source IP based filtering) or other restrictions (such as quotas), attackers may circumvent those limits in such a scenario by using the Directory Traversal to retrieve data from the other instances. If the associated XMPP server (or anyone knowing the SECRET_KEY) is malicious, they can write files outside the DATA_ROOT. The files which are written are constrained to have the `.meta` and the `.data` suffixes; the `.meta` file will contain the JSON with the Content-Type of the original request and the `.data` file will contain the payload. The issue is patched in version 0.4.0.	3.5	More Details
CVE-2020-1905	Media ContentProvider URIs used for opening attachments in other apps were generated sequentially prior to WhatsApp for Android v2.20.185, which could have allowed a malicious third party app chosen to open the file to guess the URIs for previously opened attachments until the opener app is terminated.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14378	An integer underflow in dpdk versions before 18.11.10 and before 19.11.5 in the `move_desc` function can lead to large amounts of CPU cycles being eaten up in a long running loop. An attacker could cause `move_desc` to get stuck in a 4,294,967,295-count iteration loop. Depending on how `vhost_crypto` is being used this could prevent other VMs or network tasks from being serviced by the busy DPDK lcore for an extended period.	3.3	More Details
CVE-2020-4629	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a local user with specialized access to obtain sensitive information from a detailed technical error message. This information could be used in further attacks against the system. IBM X-Force ID: 185370.	3.3	More Details
CVE-2020-25741	fdctrl_write_data in hw/block/fdc.c in QEMU 5.0.0 has a NULL pointer dereference via a NULL block pointer for the current drive.	3.2	More Details
CVE-2020-25743	hw/ide/pci.c in QEMU before 5.1.1 can trigger a NULL pointer dereference because it lacks a pointer check before an ide_cancel_dma_sync call.	3.2	More Details
CVE-2020-25742	pci_change_irq_level in hw/pci/pci.c in QEMU before 5.1.1 has a NULL pointer dereference because pci_get_bus() might not return a valid pointer.	3.2	More Details
CVE-2020-15731	An improper Input Validation vulnerability in the code handling file renaming and recovery in Bitdefender Engines allows an attacker to write an arbitrary file in a location hardcoded in a specially-crafted malicious file name. This issue affects: Bitdefender Engines versions prior to 7.85448.	3.2	More Details
CVE-2020-15671	When typing in a password under certain conditions, a race may have occured where the InputContext was not being correctly set for the input field, resulting in the typed password being saved to the keyboard dictionary. This vulnerability affects Firefox for Android < 80.	3.1	More Details
CVE-2020-5387	Dell XPS 13 9370 BIOS versions prior to 1.13.1 contains an Improper Exception Handling vulnerability. A local attacker with physical access could exploit this vulnerability to prevent the system from booting until the exploited boot device is removed.	2.3	More Details
CVE-2020-26053	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 Number	Description	Base Score	Reference
CVE-2020-13506	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2020-26159	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details