SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 May 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-2019-15874	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in memory access after it has been freed leading to a kernel panic or other unpredictable results.	9.8	More Details
CVE-2019-5623	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').	9.8	More Details
CVE-2020-12641	rcube_image.php in Roundcube Webmail before 1.4.4 allows attackers to execute arbitrary code via shell metacharacters in a configuration setting for im_convert_path or im_identify_path.	9.8	More Details
CVE-2020-12640	Roundcube Webmail before 1.4.4 allows attackers to include local files and execute code via directory traversal in a plugin name to rcube_plugin_api.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8790	The OKLOK (3.1.1) mobile companion app for Fingerprint Bluetooth Padlock FB50 (2.3) has weak password requirements combined with improper restriction of excessive authentication attempts, which could allow a remote attacker to discover user credentials and obtain access via a brute force attack.	9.8	More Details
CVE-2020-12110	Certain TP-Link devices have a Hardcoded Encryption Key. This affects NC200 2.1.9 build 200225, N210 1.0.9 build 200304, NC220 1.3.0 build 200304, NC230 1.3.0 build 200304, NC250 1.3.0 build 200304, NC260 1.5.2 build 200304, and NC450 1.5.3 build 200304.	9.8	More Details
CVE-2020-1961	Vulnerability to Server-Side Template Injection on Mail templates for Apache Syncope 2.0.X releases prior to 2.0.15, 2.1.X releases prior to 2.1.6, enabling attackers to inject arbitrary JEXL expressions, leading to Remote Code Execution (RCE) was discovered.	9.8	More Details
CVE-2020-1959	A Server-Side Template Injection was identified in Apache Syncope prior to 2.1.6 enabling attackers to inject arbitrary Java EL expressions, leading to an unauthenticated Remote Code Execution (RCE) vulnerability. Apache Syncope uses Java Bean Validation (JSR 380) custom constraint validators. When building custom constraint violation error messages, they support different types of interpolation, including Java EL expressions. Therefore, if an attacker can inject arbitrary data in the error message template being passed, they will be able to run arbitrary Java code.	9.8	More Details
CVE-2020-12627	Calibre-Web 0.6.6 allows authentication bypass because of the 'A0Zr98j/3yX R~XHH!jmN]LWX/,?RT' hardcoded secret key.	9.8	More Details
CVE-2020-7645	All versions of chrome-launcher allow execution of arbitrary commands, by controlling the $HOME environment variable in Linux operating systems.	9.8	More Details
CVE-2020-10683	dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.	9.8	More Details
CVE-2019-5614	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in accessing out-of-bounds memory leading to a kernel panic or other unpredictable results.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11651	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.	9.8	More Details
CVE-2020-7136	A security vulnerability in HPE Smart Update Manager (SUM) prior to version 8.5.6 could allow remote unauthorized access. Hewlett Packard Enterprise has provided a software update to resolve this vulnerability in HPE Smart Update Manager (SUM) prior to 8.5.6. Please visit the HPE Support Center at https://support.hpe.com/hpesc/public/home to download the latest version of HPE Smart Update Manager (SUM). Download the latest version of HPE Smart Update Manager (SUM) or download the latest Service Pack For ProLiant (SPP).	9.8	More Details
CVE-2019-5622	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-798: Use of Hard-coded Credentials.	9.8	More Details
CVE-2019-5619	AASync.com AASync version 2.2.1.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	9.8	More Details
CVE-2020-12443	BigBlueButton before 2.2.6 allows remote attackers to read arbitrary files because the presfilename (lowercase) value can be a .pdf filename while the presFilename (mixed case) value has a ../ sequence. This can be leveraged for privilege escalation via a directory traversal to bigbluebutton.properties. NOTE: this issue exists because of an ineffective mitigation to CVE-2020-12112 in which there was an attempted fix within an NGINX configuration file, without considering that the relevant part of NGINX is case-insensitive.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8481	For ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, confidential data is written in an unprotected file. An attacker who successfully exploited this vulnerability could take full control of the computer.	9.8	More Details
CVE-2020-12471	MonoX through 5.1.40.5152 allows remote code execution via HTML5Upload.ashx or Pages/SocialNetworking/lng/en-US/PhotoGallery.aspx because of deserialization in ModuleGallery.HTML5Upload, ModuleGallery.SilverLightUploadModule, HTML5Upload, and SilverLightUploadHandler.	9.8	More Details
CVE-2016-11061	Xerox WorkCentre 3655, 3655i, 58XX, 58XXi, 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi, 78XX, 78XXi, 7970, and 7970i devices before 073.xxx.086.15410 do not properly escape parameters in the support/remoteUI/configrui.php script, which can allow an unauthenticated attacker to execute OS commands on the device.	9.8	More Details
CVE-2019-5620	ABB MicroSCADA Pro SYS600 version 9.3 suffers from an instance of CWE-306: Missing Authentication for Critical Function.	9.8	More Details
CVE-2020-11942	An issue was discovered in Open-AudIT 3.2.2. There are Multiple SQL Injections.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8479	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, ABB AbilityTM SCADAvantage versions 5.1 to 5.6.5. an XML External Entity Injection vulnerability exists that allows an attacker to read or call arbitrary files from the license server and/or from the network and also block the license handling.	9.4	More Details
CVE-2020-3955	ESXi 6.5 without patch ESXi650-201912104-SG and ESXi 6.7 without patch ESXi670-202004103-SG do not properly neutralize script-related HTML when viewing virtual machines attributes. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.3.	9.3	More Details
CVE-2020-11016	IntelMQ Manager from version 1.1.0 and before version 2.1.1 has a vulnerability where the backend incorrectly handled messages given by user-input in the "send" functionality of the Inspect-tool of the Monitor component. An attacker with access to the IntelMQ Manager could possibly use this issue to execute arbitrary code with the privileges of the webserver. Version 2.1.1 fixes the vulnerability.	9.1	More Details
CVE-2020-5887	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for remote attackers to access local daemons and bypass port lockdown settings.	9.1	More Details
CVE-2020-5886	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems setup for connection mirroring in a High Availability (HA) pair transfers sensitive cryptographic objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	9.1	More Details
CVE-2020-5885	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems set up for connection mirroring in a high availability (HA) pair transfer sensitive cryptographic objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5884	On versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.4, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the default deployment mode for BIG-IP high availability (HA) pair mirroring is insecure. This is a control plane issue that is exposed only on the network used for mirroring.	9.1	More Details
CVE-2020-7452	In FreeBSD 12.1-STABLE before r357490, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r357489, and 11.3-RELEASE before 11.3-RELEASE-p7, incorrect use of a user-controlled pointer in the epair virtual network module allowed vnet jailed privileged users to panic the host system and potentially execute arbitrary code in the kernel.	9.1	More Details
CVE-2020-10634	SAE IT-systems FW-50 Remote Telemetry Unit (RTU). A specially crafted request could allow an attacker to view the file structure of the affected device and access files that should be inaccessible.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-8775	Pega Platform before version 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability in the comment tags.	8.9	More Details
CVE-2020-8773	The Richtext Editor in Pega Platform before 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability.	8.9	More Details
CVE-2019-19216	BMC Control-M/Agent 7.0.00.000 has an Insecure File Copy.	8.8	More Details
CVE-2020-12479	TeamPass 2.1.27.36 allows any authenticated TeamPass user to trigger a PHP file include vulnerability via a crafted HTTP request with sources/users.queries.php newValue directory traversal.	8.8	More Details
CVE-2019-19220	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection (issue 2 of 2).	8.8	More Details
CVE-2020-8829	CSRF on Intelbras CIP 92200 devices allows an attacker to access the panel and perform scraping or other analysis.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12246	Beeline Smart Box 2.0.38 routers allow "Advanced settings > Other > Diagnostics" OS command injection via the Ping ping_ipaddr parameter, the Nslookup nslookup_ipaddr parameter, or the Traceroute traceroute_ipaddr parameter.	8.8	More Details
CVE-2020-5331	RSA Archer, versions prior to 6.7 P3 (6.7.0.3), contain an information exposure vulnerability. Users' session information could potentially be stored in cache or log files. An authenticated malicious local user with access to the log files may obtain the exposed information to use it in further attacks.	8.8	More Details
CVE-2017-18855	NETGEAR WNR854T devices before 1.5.2 are affected by command execution.	8.8	More Details
CVE-2020-8774	Pega Platform before version 8.2.6 is affected by a Reflected Cross-Site Scripting vulnerability in the "ActionStringID" function.	8.8	More Details
CVE-2020-11675	Cerner medico 26.00 has a Local Buffer Overflow (issue 1 of 3).	8.8	More Details
CVE-2019-16653	An application plugin in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to gain admin privileges.	8.8	More Details
CVE-2019-19217	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection.	8.8	More Details
CVE-2020-8830	CSRF in login.asp on Ruckus devices allows an attacker to access the panel, and use SSRF to perform scraping or other analysis via the SUBCA-1 field on the Wireless Admin screen.	8.8	More Details
CVE-2020-11677	Cerner medico 26.00 has a Local Buffer Overflow (issue 3 of 3).	8.8	More Details
CVE-2020-11676	Cerner medico 26.00 has a Local Buffer Overflow (issue 2 of 3).	8.8	More Details
CVE-2020-12109	Certain TP-Link devices allow Command Injection. This affects NC200 2.1.9 build 200225, NC210 1.0.9 build 200304, NC220 1.3.0 build 200304, NC230 1.3.0 build 200304, NC250 1.3.0 build 200304, NC260 1.5.2 build 200304, and NC450 1.5.3 build 200304.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12111	Certain TP-Link devices allow Command Injection. This affects NC260 1.5.2 build 200304 and NC450 1.5.3 build 200304.	8.8	More Details
CVE-2020-12461	PHP-Fusion 9.03.50 allows SQL Injection because maincore.php has an insufficient protection mechanism. An attacker can develop a crafted payload that can be inserted into the sort_order GET parameter on the members.php members search page. This parameter allows for control over anything after the ORDER BY clause in the SQL query.	8.8	More Details
CVE-2019-19517	Intelbras RF1200 1.1.3 devices allow CSRF to bypass the login.html form, as demonstrated by launching a scrapy process.	8.8	More Details
CVE-2019-19215	A buffer overflow vulnerability in BMC Control-M/Agent 7.0.00.000 when the On-Do action destination is Mail and the Control-M/Agent is configured to send the email, allows remote attackers to have unspecified impact via vectors related to the configured IP address or SMTP server.	8.8	More Details
CVE-2020-12104	The Import feature in the wp-advanced-search plugin 3.3.6 for WordPress is vulnerable to authenticated SQL injection via an uploaded .sql file. An attacker can use this to execute SQL commands without any validation.	8.8	More Details
CVE-2019-0235	Apache OFBiz 17.12.01 is vulnerable to some CSRF attacks.	8.8	More Details
CVE-2020-6010	LearnPress Wordpress plugin version prior and including 3.2.6.7 is vulnerable to SQL Injection	8.8	More Details
	A vulnerability in the HTTP/HTTPS service used by J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Zero Touch Provisioning (ZTP) allows an unauthenticated attacker to perform local file inclusion (LFI) or path traversal. Using this vulnerability, an attacker may be able to inject commands into the httpd.log, read files with 'world' readable permission file or obtain J-Web session tokens. In the case of command injection, as the HTTP service runs as user 'nobody', the impact of this command injection is limited. (CVSS score 5.3, vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) In the case of reading files with 'world' readable permission, in Junos OS 19.3R1 and above, the unauthenticated attacker would be able to read the configuration file. (CVSS score 5.9, vector CVSS:3.1/ AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N) If J-Web is enabled, the attacker could gain the same level of access of anyone actively logged into J-Web. If an administrator is logged in, the attacker could gain administrator		

CVE Number	Description	Base Score	Reference
	access to J-Web. (CVSS score 8.8, vector CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) This issue only affects Juniper Networks Junos OS devices with HTTP/HTTPS services enabled. Junos OS devices with HTTP/HTTPS services disabled are not affected. If HTTP/HTTPS services are enabled, the following command will show the httpd processes: user@device> show system processes	match http 5260 - S 0:00.13 /usr/sbin/httpd-gk -N 5797 - I 0:00.10 /usr/sbin/httpd --config /jail/var/etc/httpd.conf To summarize: If HTTP/HTTPS services are disabled, there is no impact from this vulnerability. If HTTP/HTTPS services are enabled and J-Web is not in use, this vulnerability has a CVSS score of 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). If J-Web is enabled, this vulnerability has a CVSS score of 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H). Juniper SIRT has received a single report of this vulnerability being exploited in the wild. Out of an abundance of caution, we are notifying customers so they can take appropriate actions. Indicators of Compromise: The /var/log/httpd.log may have indicators that commands have injected or files being accessed. The device administrator can look for these indicators by searching for the string patterns "=*;*&" or "*%3b*&" in /var/log/httpd.log, using the following command: user@device> show log httpd.log	match "=*;*&|=*%3b*&" If this command returns any output, it might be an indication of malicious attempts or simply scanning activities. Rotated logs should also be reviewed, using the following command: user@device> show log httpd.log.0.gz	match "=*;*&|=*%3b*&" user@device> show log httpd.log.1.gz	match "=*;*&|=*%3b*&" Note that a skilled attacker would likely remove these entries from the local log file, thus effectively eliminating any reliable signature that the device had been attacked. This issue affects Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D101, 12.3X48-D105; 14.1X53 versions prior to 14.1X53-D54; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D211, 15.1X49-D220; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S4; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R3-S2 ; 18.4 version 18.4R2 and later versions; 19.1 versions prior to 19.1R1-S5, 19.1R3-S1; 19.1 version 19.1R2 and later versions; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2; 20.1 versions prior to 20.1R1-S1, 20.1R2.	8.8	More Details
CVE-2020-11674	Cerner medico 26.00 allows variable reuse, possibly causing data corruption.	8.8	More Details
CVE-2020-11943	An issue was discovered in Open-AudIT 3.2.2. There is Arbitrary file upload.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18864	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R6900P before 1.0.0.56, R7100LG before 1.0.0.32, R7300 before 1.0.0.54, R7900 before 1.0.1.18, R8300 before 1.0.2.104, and R8500 before 1.0.2.104.	8.8	More Details
CVE-2020-11026	In affected versions of WordPress, files with a specially crafted name when uploaded to the Media section can lead to script execution upon accessing the file. This requires an authenticated user with privileges to upload files. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	8.7	More Details
CVE-2019-11823	CRLF injection vulnerability in Network Center in Synology Router Manager (SRM) before 1.2.3-8017-2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic.	8.6	More Details
CVE-2020-11020	Faye (NPM, RubyGem) versions greater than 0.5.0 and before 1.0.4, 1.1.3 and 1.2.5, has the potential for authentication bypass in the extension system. The vulnerability allows any client to bypass checks put in place by server-side extensions, by appending extra segments to the message channel. It is patched in versions 1.0.4, 1.1.3 and 1.2.5.	8.5	More Details
CVE-2020-8018	A Incorrect Default Permissions vulnerability in the SLES15-SP1-CHOST-BYOS and SLES15-SP1-CAP-Deployment-BYOS images of SUSE Linux Enterprise Server 15 SP1 allows local attackers with the UID 1000 to escalate to root due to a /etc directory owned by the user This issue affects: SUSE Linux Enterprise Server 15 SP1 SLES15-SP1-CAP-Deployment-BYOS version 1.0.1 and prior versions; SLES15-SP1-CHOST-BYOS versions prior to 1.0.3 and prior versions;	8.4	More Details
CVE-2020-5334	RSA Archer, versions prior to 6.7 P2 (6.7.0.2), contains a Document Object Model (DOM) based cross-site scripting vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or JavaScript code to DOM environment in the browser. The malicious code is then executed by the web browser in the context of the vulnerable web application.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5876	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, a race condition exists where mcpd and other processes may make unencrypted connection attempts to a new configuration sync peer. The race condition can occur when changing the ConfigSync IP address of a peer, adding a new peer, or when the Traffic Management Microkernel (TMM) first starts up.	8.1	More Details
CVE-2020-7983	A CSRF issue in login.asp on Ruckus R500 3.4.2.0.384 devices allows remote attackers to access the panel or conduct SSRF attacks.	8.1	More Details
CVE-2020-5888	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for adjacent network (layer 2) attackers to access local daemons and bypass port lockdown settings.	8.1	More Details
CVE-2020-11671	Lack of authorization controls in REST API functions in TeamPass through 2.1.27.36 allows any TeamPass user with a valid API token to become a TeamPass administrator and read/modify all passwords via authenticated api/index.php REST API calls. NOTE: the API is not available by default.	8.1	More Details
CVE-2020-11443	The Zoom IT installer for Windows (ZoomInstallerFull.msi) prior to version 4.6.10 deletes files located in %APPDATA%\Zoom before installing an updated version of the client. Standard users are able to write to this directory, and can write links to other directories on the machine. As the installer runs with SYSTEM privileges and follows these links, a user can cause the installer to delete files that otherwise cannot be deleted by the user.	8.1	More Details
CVE-2020-11446	ESET Antivirus and Antispyware Module module 1553 through 1560 allows a user with limited access rights to create hard links in some ESET directories and then force the product to write through these links into files that would normally not be write-able by the user, thus achieving privilege escalation.	7.8	More Details
CVE-2019-16011	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges.	7.8	More Details
CVE-2020-12468	Subrion CMS 4.2.1 allows CSV injection via a phrase value within a language. This is related to phrases/add/ and languages/download/.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8471	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, weak file permissions allow an authenticated attacker to block the license handling, escalate his/her privileges and execute arbitrary code.	7.8	More Details
CVE-2020-12463	An elevation of privilege vulnerability exists in Avira Software Updater before 2.0.6.27476 due to improperly handling file hard links. This allows local users to obtain take control of arbitrary files.	7.8	More Details
CVE-2020-8484	Insufficient protection of the inter-process communication functions in ABB System 800xA for DCI (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	7.8	More Details
CVE-2020-8485	Insufficient protection of the inter-process communication functions in ABB System 800xA for MOD 300 (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	7.8	More Details
CVE-2020-8488	Insufficient protection of the inter-process communication functions in ABB System 800xA Batch Management (all published versions) enables an attacker authenticated on the local system to inject data, affecting User Interface update during batch execution and/or compare/printing functionalities.	7.8	More Details
CVE-2020-1817	Huawei PCManager with versions earlier than 10.0.1.36 has a privilege escalation vulnerability. Due to improper permission management of specific files, local attackers with low permissions can inject commands to exploit this vulnerability. Successful exploit may cause privilege escalation.	7.8	More Details
CVE-2020-8489	Insufficient protection of the inter-process communication functions in ABB System 800xA Information Management (all published versions) enables an attacker authenticated on the local system to inject data, affecting the runtime values to be stored in the archive, or making Information Management history services unavailable.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5621	ABBS Software Audio Media Player version 3.1 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	7.8	More Details
CVE-2020-10622	LCDS LAquis SCADA Versions 4.3.1 and prior. The affected product is vulnerable to arbitrary file creation by unauthorized users	7.8	More Details
CVE-2019-5618	A-PDF WAV to MP3 version 1.0.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	7.8	More Details
CVE-2019-20781	An issue was discovered in LG Bridge before April 2019 on Windows. DLL Hijacking can occur.	7.8	More Details
CVE-2020-12657	An issue was discovered in the Linux kernel before 5.6.5. There is a use-after-free in block/bfq-iosched.c related to bfq_idle_slice_timer_body.	7.8	More Details
CVE-2020-12653	An issue was found in Linux kernel before 5.5.4. The mwifiex_cmd_append_vsie_tlv() function in drivers/net/wireless/marvell/mwifiex/scan.c allows local users to gain privileges or cause a denial of service because of an incorrect memcpy and buffer overflow, aka CID-b70261a288ea.	7.8	More Details
CVE-2020-12446	The ene.sys driver in G.SKILL Trident Z Lighting Control through 1.00.08 exposes mapping and un-mapping of physical memory, reading and writing to Model Specific Register (MSR) registers, and input from and output to I/O ports to local non-privileged users. This leads to privilege escalation to NT AUTHORITY\SYSTEM.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18860	Certain NETGEAR devices are affected by debugging command execution. This affects FS752TP 5.4.2.19 and earlier, GS108Tv2 5.4.2.29 and earlier, GS110TP 5.4.2.29 and earlier, GS418TPP 6.6.2.6 and earlier, GS510TLP 6.6.2.6 and earlier, GS510TP 5.04.2.27 and earlier, GS510TPP 6.6.2.6 and earlier, GS716Tv2 5.4.2.27 and earlier, GS716Tv3 6.3.1.16 and earlier, GS724Tv3 5.4.2.27 and earlier, GS724Tv4 6.3.1.16 and earlier, GS728TPSB 5.3.0.29 and earlier, GS728TSB 5.3.0.29 and earlier, GS728TXS 6.1.0.35 and earlier, GS748Tv4 5.4.2.27 and earlier, GS748Tv5 6.3.1.16 and earlier, GS752TPSB 5.3.0.29 and earlier, GS752TSB 5.3.0.29 and earlier, GS752TXS 6.1.0.35 and earlier, M4200 12.0.2.10 and earlier, M4300 12.0.2.10 and earlier, M5300 11.0.0.28 and earlier, M6100 11.0.0.28 and earlier, M7100 11.0.0.28 and earlier, S3300 6.6.1.4 and earlier, XS708T 6.6.0.11 and earlier, XS712T 6.1.0.34 and earlier, and XS716T 6.6.0.11 and earlier.	7.7	More Details
CVE-2020-11036	In GLPI before version 9.4.6 there are multiple related stored XSS vulnerabilities. The package is vulnerable to Stored XSS in the comments of items in the Knowledge base. Adding a comment with content "<script>alert(1)</script>" reproduces the attack. This can be exploited by a user with administrator privileges in the User-Agent field. It can also be exploited by an outside party through the following steps: 1. Create a user with the surname `" onmouseover="alert(document.cookie)` and an empty first name. 2. With this user, create a ticket 3. As an administrator (or other privileged user) open the created ticket 4. On the "last update" field, put your mouse on the name of the user 5. The XSS fires This is fixed in version 9.4.6.	7.6	More Details
CVE-2020-11032	In GLPI before version 9.4.6, there is a SQL injection vulnerability for all helpdesk instances. Exploiting this vulnerability requires a technician account. This is fixed in version 9.4.6.	7.6	More Details
CVE-2019-19219	BMC Control-M/Agent 7.0.00.000 allows Arbitrary File Download.	7.5	More Details
CVE-2019-19218	BMC Control-M/Agent 7.0.00.000 has Insecure Password Storage.	7.5	More Details
CVE-2020-11015	A vulnerability has been disclosed in thinx-device-api IoT Device Management Server before version 2.5.0. Device MAC address can be spoofed. This means initial registration requests without UDID and spoofed MAC address may pass to create new UDID with same MAC address. Full impact needs to be reviewed further. Applies to all (mostly ESP8266/ESP32) users. This has been fixed in firmware version 2.5.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5871	On BIG-IP 14.1.0-14.1.2.3, undisclosed requests can lead to a denial of service (DoS) when sent to BIG-IP HTTP/2 virtual servers. The problem can occur when ciphers, which have been blacklisted by the HTTP/2 RFC, are used on backend servers. This is a data-plane issue. There is no control-plane exposure.	7.5	More Details
CVE-2019-12425	Apache OFBiz 17.12.01 is vulnerable to Host header injection by accepting arbitrary host	7.5	More Details
CVE-2020-5891	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, undisclosed HTTP/2 requests can lead to a denial of service when sent to a virtual server configured with the Fallback Host setting and a server-side HTTP/2 profile.	7.5	More Details
CVE-2020-5872	On BIG-IP 14.1.0-14.1.2.3, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.4.1, when processing TLS traffic with hardware cryptographic acceleration enabled on platforms with Intel QAT hardware, the Traffic Management Microkernel (TMM) may stop responding and cause a failover event.	7.5	More Details
CVE-2020-5874	On BIG-IP APM 15.0.0-15.0.1.2, 14.1.0-14.1.2.3, and 14.0.0-14.0.1, in certain circumstances, an attacker sending specifically crafted requests to a BIG-IP APM virtual server may cause a disruption of service provided by the Traffic Management Microkernel(TMM).	7.5	More Details
CVE-2020-5875	On BIG-IP 15.0.0-15.0.1 and 14.1.0-14.1.2.3, under certain conditions, the Traffic Management Microkernel (TMM) may generate a core file and restart while processing SSL traffic with an HTTP/2 full proxy.	7.5	More Details
CVE-2020-5877	On BIG-IP 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, malformed input to the DATAGRAM::tcp iRules command within a FLOW_INIT event may lead to a denial of service.	7.5	More Details
CVE-2020-5878	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.3, Traffic Management Microkernel (TMM) may restart on BIG-IP Virtual Edition (VE) while processing unusual IP traffic.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5879	On BIG-IP ASM 11.6.1-11.6.5.1, under certain configurations, the BIG-IP system sends data plane traffic to back-end servers unencrypted, even when a Server SSL profile is applied.	7.5	More Details
CVE-2020-5881	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when the BIG-IP Virtual Edition (VE) is configured with VLAN groups and there are devices configured with OSPF connected to it, the Network Device Abstraction Layer (NDAL) Interfaces can lock up and in turn disrupting the communication between the mcpd and tmm processes.	7.5	More Details
CVE-2020-5882	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5, and 11.6.1-11.6.5.1, under certain conditions, the Intel QuickAssist Technology (QAT) cryptography driver may produce a Traffic Management Microkernel (TMM) core file.	7.5	More Details
CVE-2020-5883	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, when a virtual server is configured with HTTP explicit proxy and has an attached HTTP_PROXY_REQUEST iRule, POST requests sent to the virtual server cause an xdata memory leak.	7.5	More Details
CVE-2020-9098	Huawei OceanStor 5310 product with version of V500R007C60SPC100 has an invalid pointer access vulnerability. The software system access an invalid pointer when attacker malformed packet. Due to the insufficient validation of some parameter, successful exploit could cause device reboot.	7.5	More Details
CVE-2020-12642	An issue was discovered in service-api before 4.3.12 and 5.x before 5.1.1 for Report Portal. It allows XXE, with resultant secrets disclosure and SSRF, via JUnit XML launch import.	7.5	More Details
CVE-2020-11462	An issue was discovered in OpenVPN Access Server before 2.7.0 and 2.8.x before 2.8.3. With the full featured RPC2 interface enabled, it is possible to achieve a temporary DoS state of the management interface when sending an XML Entity Expansion (XEE) payload to the XMLRPC based RPC2 interface. The duration of the DoS state depends on available memory and CPU speed. The default restricted mode of the RPC2 interface is NOT vulnerable.	7.5	More Details
CVE-2020-11842	Information disclosure vulnerability in Micro Focus Verastream Host Integrator (VHI) product, affecting versions earlier than 7.8 Update 1 (7.8.49 or 7.8.0.49). The vulnerability allows an unauthenticated attackers to view information they may not have been authorized to view.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10876	The OKLOK (3.1.1) mobile companion app for Fingerprint Bluetooth Padlock FB50 (2.3) does not correctly implement its timeout on the four-digit verification code that is required for resetting passwords, nor does it properly restrict excessive verification attempts. This allows an attacker to brute force the four-digit verification code in order to bypass email verification and change the password of a victim account.	7.5	More Details
CVE-2020-12649	Gurbalib through 2020-04-30 allows lib/cmds/player/help.c directory traversal for reading administrative paths.	7.5	More Details
CVE-2020-12478	TeamPass 2.1.27.36 allows an unauthenticated attacker to retrieve files from the TeamPass web root. This may include backups or LDAP debug files.	7.5	More Details
CVE-2019-13285	CoSoSys Endpoint Protector 5.1.0.2 allows Host Header Injection.	7.5	More Details
CVE-2020-11035	In GLPI after version 0.83.3 and before version 9.4.6, the CSRF tokens are generated using an insecure algorithm. The implementation uses rand and uniqid and MD5 which does not provide secure values. This is fixed in version 9.4.6.	7.5	More Details
CVE-2020-2575	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2019-19100	A privilege escalation vulnerability in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.4SP, <. 4.6.3SP, < 4.7.2 and < 4.8.1 allow authenticated users to delete arbitrary files via an exposed interface.	7.5	More Details
CVE-2020-12447	A Local File Inclusion (LFI) issue on Onkyo TX-NR585 1000-0000-000-0008-0000 devices allows remote unauthenticated users on the network to read sensitive files via %2e%2e%2f directory traversal, as demonstrated by reading /etc/shadow.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10187	Doorkeeper version 5.0.0 and later contains an information disclosure vulnerability that allows an attacker to retrieve the client secret only intended for the OAuth application owner. After authorizing the application and allowing access, the attacker simply needs to request the list of their authorized applications in a JSON format (usually GET /oauth/authorized_applications.json). An application is vulnerable if the authorized applications controller is enabled.	7.5	More Details
CVE-2020-12477	The REST API functions in TeamPass 2.1.27.36 allow any user with a valid API token to bypass IP address whitelist restrictions via an X-Forwarded-For client HTTP header to the getIp function.	7.5	More Details
CVE-2020-8473	Insufficient folder permissions used by system functions in ABB System 800xA Base (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploit the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	7.3	More Details
CVE-2020-5343	Dell Client platforms restored using a Dell OS recovery image downloaded before December 20, 2019, may contain an insecure inherited permissions vulnerability. A local authenticated malicious user with low privileges could exploit this vulnerability to gain unauthorized access on the root folder.	7.3	More Details
CVE-2020-7351	An OS Command Injection vulnerability in the endpoint_devicemap.php component of Fonality Trixbox Community Edition allows an attacker to execute commands on the underlying operating system as the "asterisk" user. Note that Trixbox Community Edition has been unsupported by the vendor since 2012. This issue affects: Fonality Trixbox Community Edition, versions 1.2.0 through 2.8.0.4. Versions 1.0 and 1.1 are unaffected.	7.3	More Details
CVE-2020-5873	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.1-11.6.5 and BIG-IQ 5.2.0-7.1.0, a user associated with the Resource Administrator role who has access to the secure copy (scp) utility but does not have access to Advanced Shell (bash) can execute arbitrary commands using a maliciously crafted scp request.	7.2	More Details
CVE-2020-12473	MonoX through 5.1.40.5152 allows admins to execute arbitrary programs by reconfiguring the Converter Executable setting from ffmpeg.exe to a different program.	7.2	More Details
CVE-2019-16652	The BPM component in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to execute arbitrary commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19165	AxECM.cab(ActiveX Control) in Inogard Ebiz4u contains a vulnerability that could allow remote files to be downloaded and executed by setting arguments to the activeX method. Download of Code Without Integrity Check vulnerability in ActiveX control of Inogard Co,,LTD Ebiz4u ActiveX of Inogard Co,,LTD(AxECM.cab) allows ATTACKER to cause a file download to Windows user's folder and execute. This issue affects: Inogard Co,,LTD Ebiz4u ActiveX of Inogard Co,,LTD(AxECM.cab) version 1.0.5.0 and later versions on windows 7/8/10.	7.2	More Details
CVE-2020-5332	RSA Archer, versions prior to 6.7 P3 (6.7.0.3), contain a command injection vulnerability. AN authenticated malicious user with administrator privileges could potentially exploit this vulnerability to execute arbitrary commands on the system where the vulnerable application is deployed.	7.2	More Details
CVE-2020-12470	MonoX through 5.1.40.5152 allows administrators to execute arbitrary code by modifying an ASPX template.	7.2	More Details
CVE-2020-5880	Om BIG-IP 15.0.0-15.0.1.3 and 14.1.0-14.1.2.3, the restjavad process may expose a way for attackers to upload arbitrary files on the BIG-IP system, bypassing the authorization system. Resulting error messages may also reveal internal paths of the server.	7.1	More Details
CVE-2020-12654	An issue was found in Linux kernel before 5.5.4. mwifiex_ret_wmm_get_status() in drivers/net/wireless/marvell/mwifiex/wmm.c allows a remote AP to trigger a heap-based buffer overflow because of an incorrect memcpy, aka CID-3a9b153c5591.	7.1	More Details
CVE-2020-11884	In the Linux kernel 4.19 through 5.6.7 on the s390 platform, code execution may occur because of a race condition, as demonstrated by code in enable_sacf_uaccess in arch/s390/lib/uaccess.c that fails to protect against a concurrent page table upgrade, aka CID-3f777e19d171. A crash could also occur.	7.0	More Details
CVE-2020-1752	A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.	7.0	More Details
CVE-2020-12050	SQLiteODBC 0.9996, as packaged for certain Linux distributions as 0.9996-4, has a race condition leading to root privilege escalation because any user can replace a /tmp/sqliteodbc$$ file with new contents that cause loading of an arbitrary library.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	6.9	More Details
CVE-2020-11051	In Wiki.js before 2.3.81, there is a stored XSS in the Markdown editor. An editor with write access to a page, using the Markdown editor, could inject an XSS payload into the content. If another editor (with write access as well) load the same page into the Markdown editor, the XSS payload will be executed as part of the preview panel. The rendered result does not contain the XSS payload as it is stripped by the HTML Sanitization security module. This vulnerability only impacts editors loading the malicious page in the Markdown editor. This has been patched in 2.3.81.	6.9	More Details
CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	6.9	More Details
CVE-2020-8157	UniFi Cloud Key firmware <= v1.1.10 for Cloud Key gen2 and Cloud Key gen2 Plus contains a vulnerability that allows unrestricted root access through the serial interface (UART).	6.8	More Details
CVE-2017-18867	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6100 before 1.0.0.55, D7800 before V1.0.1.24, R7100LG before V1.0.0.32, WNDR4300v1 before 1.0.2.90, and WNDR4500v3 before 1.0.0.48.	6.8	More Details
CVE-2019-20792	OpenSC before 0.20.0 has a double free in coolkey_free_private_data because coolkey_add_object in libopensc/card-coolkey.c lacks a uniqueness check.	6.8	More Details
CVE-2017-18865	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8300 before 1.0.2.104 and R8500 before 1.0.2.104.	6.8	More Details
CVE-2020-12659	An issue was discovered in the Linux kernel before 5.6.7. xdp_umem_reg in net/xdp/xdp_umem.c has an out-of-bounds write (by a user with the CAP_NET_ADMIN capability) because of a lack of headroom validation.	6.7	More Details
CVE-2020-5892	In versions 7.1.5-7.1.8, the BIG-IP Edge Client components in BIG-IP APM, Edge Gateway, and FirePass legacy allow attackers to obtain the full session ID from process memory.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12464	usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference, aka CID-056ad39ee925.	6.7	More Details
CVE-2020-12465	An array overflow was discovered in mt76_add_fragment in drivers/net/wireless/mediatek/mt76/dma.c in the Linux kernel before 5.5.10, aka CID-b102f0c522cf. An oversized packet with too many rx fragments can corrupt memory of adjacent pages.	6.7	More Details
CVE-2017-18856	NETGEAR ReadyNAS devices before 6.6.1 are affected by command injection.	6.7	More Details
CVE-2017-18854	NETGEAR ReadyNAS 6.6.1 and earlier is affected by command injection.	6.7	More Details
CVE-2020-8487	Insufficient protection of the inter-process communication functions in ABB System 800xA Base (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	6.6	More Details
CVE-2020-8486	Insufficient protection of the inter-process communication functions in ABB System 800xA RNRP (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	6.6	More Details
CVE-2020-11033	In GLPI from version 9.1 and before version 9.4.6, any API user with READ right on User itemtype will have access to full list of users when querying apirest.php/User. The response contains: - All api_tokens which can be used to do privileges escalations or read/update/delete data normally non accessible to the current user. - All personal_tokens can display another users planning. Exploiting this vulnerability requires the api to be enabled, a technician account. It can be mitigated by adding an application token. This is fixed in version 9.4.6.	6.6	More Details
CVE-2020-12626	An issue was discovered in Roundcube Webmail before 1.4.4. A CSRF attack can cause an authenticated user to be logged out because POST was not considered.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8791	The OKLOK (3.1.1) mobile companion app for Fingerprint Bluetooth Padlock FB50 (2.3) allows remote attackers to submit API requests using authenticated but unauthorized tokens, resulting in IDOR issues. A remote attacker can use their own token to make unauthorized API requests on behalf of arbitrary user IDs. Valid and current user IDs are trivial to guess because of the user ID assignment convention used by the app. A remote attacker could harvest email addresses, unsalted MD5 password hashes, owner-assigned lock names, and owner-assigned fingerprint names for any range of arbitrary user IDs.	6.5	More Details
CVE-2018-21233	TensorFlow before 1.7.0 has an integer overflow that causes an out-of-bounds read, possibly causing disclosure of the contents of process memory. This occurs in the DecodeBmp feature of the BMP decoder in core/kernels/decode_bmp_op.cc.	6.5	More Details
CVE-2019-19101	A missing secure communication definition and an incomplete TLS validation in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.5SP, < 4.6.4 and < 4.7.2 enable unauthenticated users to perform MITM attacks via the B&R upgrade server.	6.5	More Details
CVE-2020-12474	Telegram Desktop through 2.0.1, Telegram through 6.0.1 for Android, and Telegram through 6.0.1 for iOS allow an IDN Homograph attack via Punycode in a public URL or a group chat invitation URL.	6.5	More Details
CVE-2020-12624	The League application before 2020-05-02 on Android sends a bearer token in an HTTP Authorization header to an arbitrary web site that hosts an external image because an OkHttp object is reused, which allows remote attackers to hijack sessions.	6.5	More Details
CVE-2020-10859	Zoho ManageEngine Desktop Central before 10.0.484 allows authenticated arbitrary file writes during ZIP archive extraction via Directory Traversal in a crafted AppDependency API request.	6.5	More Details
CVE-2020-5517	CSRF in the /login URI in BlueOnyx 5209R allows an attacker to access the dashboard and perform scraping or other analysis.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11009	In Rundeck before version 3.2.6, authenticated users can craft a request that reveals Execution data and logs and Job details that they are not authorized to see. Depending on the configuration and the way that Rundeck is used, this could result in anything between a high severity risk, or a very low risk. If access is tightly restricted and all users on the system have access to all projects, this is not really much of an issue. If access is wider and allows login for users that do not have access to any projects, or project access is restricted, there is a larger issue. If access is meant to be restricted and secrets, sensitive data, or intellectual property are exposed in Rundeck execution output and job data, the risk becomes much higher. This vulnerability is patched in version 3.2.6	6.5	More Details
CVE-2020-6865	ZTE SDN controller platform is impacted by an information leakage vulnerability. Due to the program's failure to optimize the response of failure to the request, the caller can directly view the internal error code location of the component. Attackers could exploit this vulnerability to obtain sensitive information. This affects: OSCP versions V16.19.10 and V16.19.20.	6.5	More Details
CVE-2020-11652	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.	6.5	More Details
CVE-2020-12469	admin/blocks.php in Subrion CMS through 4.2.1 allows PHP Object Injection (with resultant file deletion) via serialized data in the subpages value within a block to blocks/edit.	6.5	More Details
CVE-2020-12467	Subrion CMS 4.2.1 allows session fixation via an alphanumeric value in a session cookie.	6.5	More Details
CVE-2017-18853	Certain NETGEAR devices are affected by password recovery and file access. This affects D8500 1.0.3.27 and earlier, DGN2200v4 1.0.0.82 and earlier, R6300v2 1.0.4.06 and earlier, R6400 1.0.1.20 and earlier, R6400v2 1.0.2.18 and earlier, R6700 1.0.1.22 and earlier, R6900 1.0.1.20 and earlier, R7000 1.0.7.10 and earlier, R7000P 1.0.0.58 and earlier, R7100LG 1.0.0.28 and earlier, R7300DST 1.0.0.52 and earlier, R7900 1.0.1.12 and earlier, R8000 1.0.3.46 and earlier, R8300 1.0.2.86 and earlier, R8500 1.0.2.86 and earlier, WNDR3400v3 1.0.1.8 and earlier, and WNDR4500v2 1.0.0.62 and earlier.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11030	In affected versions of WordPress, a special payload can be crafted that can lead to scripts getting executed within the search block of the block editor. This requires an authenticated user with the ability to add content. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	6.4	More Details
CVE-2020-7804	ActiveX Control(HShell.dll) in Handy Groupware 1.7.3.1 for Windows 7, 8, and 10 allows an attacker to execute arbitrary command via the ShellExec method.	6.4	More Details
CVE-2020-11021	Actions Http-Client (NPM @actions/http-client) before version 1.0.8 can disclose Authorization headers to incorrect domain in certain redirect scenarios. The conditions in which this happens are if consumers of the http-client: 1. make an http request with an authorization header 2. that request leads to a redirect (302) and 3. the redirect url redirects to another domain or hostname Then the authorization header will get passed to the other domain. The problem is fixed in version 1.0.8.	6.3	More Details
CVE-2020-12252	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an arbitrary file upload for an authenticated user. If an executable file is uploaded into the www-root directory, then it could yield remote code execution via the filename parameter.	6.2	More Details
CVE-2020-12639	phpList before 3.5.3 allows XSS, with resultant privilege elevation, via lists/admin/template.php.	6.1	More Details
CVE-2020-8033	Ruckus R500 3.4.2.0.384 devices allow XSS via the index.asp Device Name field.	6.1	More Details
CVE-2020-11034	In GLPI before version 9.4.6, there is a vulnerability that allows bypassing the open redirect protection based which is based on a regexp. This is fixed in version 9.4.6.	6.1	More Details
CVE-2019-19515	Ayision Ays-WR01 v28K.RPT.20161224 devices allow stored XSS in wireless settings.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11737	A cross-site scripting (XSS) vulnerability in Web Client in Zimbra 9.0 allows a remote attacker to craft links in an E-Mail message or calendar invite to execute arbitrary JavaScript. The attack requires an A element containing an href attribute with a "www" substring (including the quotes) followed immediately by a DOM event listener such as onmouseover. This is fixed in 9.0.0 Patch 2.	6.1	More Details
CVE-2020-10630	SAE IT-systems FW-50 Remote Telemetry Unit (RTU). The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in the output used as a webpage that is served to other users.	6.1	More Details
CVE-2017-18866	Certain NETGEAR devices are affected by stored XSS. This affects R9000 before 1.0.2.40, R6100 before 1.0.1.1, 6R7500 before 1.0.0.110, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, WNDR4300v2 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	6.1	More Details
CVE-2020-12666	macaron before 1.3.7 has an open redirect in the static handler, as demonstrated by the http://127.0.0.1:4000//example.com/ URL.	6.1	More Details
CVE-2020-12462	The ninja-forms plugin before 3.4.24.2 for WordPress allows CSRF with resultant XSS.	6.1	More Details
CVE-2019-4209	HCL Connections v5.5, v6.0, and v6.5 contains an open redirect vulnerability which could be exploited by an attacker to conduct phishing attacks.	6.1	More Details
CVE-2020-11037	In Wagtail before versions 2.7.3 and 2.8.2, a potential timing attack exists on pages or documents that have been protected with a shared password through Wagtail's "Privacy" controls. This password check is performed through a character-by-character string comparison, and so an attacker who is able to measure the time taken by this check to a high degree of accuracy could potentially use timing differences to gain knowledge of the password. This is [understood to be feasible on a local network, but not on the public internet](https://groups.google.com/d/msg/django-developers/iAaq0pvHXuA/fpUuwjK3i2wJ). Privacy settings that restrict access to pages/documents on a per-user or per-group basis (as opposed to a shared password) are unaffected by this vulnerability. This has been patched in 2.7.3, 2.8.2, 2.9.	6.1	More Details
CVE-2020-6579	Cross-site scripting (XSS) vulnerability in mailhive/cloudbeez/cloudloader.php and mailhive/cloudbeez/cloudloader_core.php in the MailBeez plugin for ZenCart before 3.9.22 allows remote attackers to inject arbitrary web script or HTML via the cloudloader_mode parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12283	Sourcegraph before 3.15.1 has a vulnerable authentication workflow because of improper validation in the SafeRedirectURL method in cmd/frontend/auth/redirect.go, such as for the //foo//example.com substring.	6.1	More Details
CVE-2020-11024	In Moonlight iOS/tvOS before 4.0.1, the pairing process is vulnerable to a man-in-the-middle attack. The bug has been fixed in Moonlight v4.0.1 for iOS and tvOS.	6.1	More Details
CVE-2020-11027	In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	6.1	More Details
CVE-2020-12625	An issue was discovered in Roundcube Webmail before 1.4.4. There is a cross-site scripting (XSS) vulnerability in rcube_washtml.php because JavaScript code can occur in the CDATA of an HTML message.	6.1	More Details
CVE-2020-10797	An XSS vulnerability resides in the hostname field of the diag_ping.php page in pfsense before 2.4.5 version. After passing inputs to the command and executing this command, the $result variable is not sanitized before it is printed.	6.1	More Details
CVE-2020-12143	The certificate used to identify Orchestrator to EdgeConnect devices is not validated, which makes it possible for someone to establish a TLS connection from EdgeConnect to an untrusted Orchestrator.	6.0	More Details
CVE-2020-12144	The certificate used to identify the Silver Peak Cloud Portal to EdgeConnect devices is not validated. This makes it possible for someone to establish a TLS connection from EdgeConnect to an untrusted portal.	6.0	More Details
CVE-2020-7453	In FreeBSD 12.1-STABLE before r359021, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r359020, and 11.3-RELEASE before 11.3-RELEASE-p7, a missing null termination check in the jail_set configuration option "osrelease" may return more bytes with a subsequent jail_get system call allowing a malicious jail superuser with permission to create nested jails to read kernel memory.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11029	In affected versions of WordPress, a vulnerability in the stats() method of class-wp-object-cache.php can be exploited to execute cross-site scripting (XSS) attacks. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	5.8	More Details
CVE-2020-11025	In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows JavaScript code to be executed. Exploitation requires an authenticated user. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	5.8	More Details
CVE-2020-11028	In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	5.8	More Details
CVE-2020-12458	An information-disclosure flaw was found in Grafana through 6.7.3. The database directory /var/lib/grafana and database file /var/lib/grafana/grafana.db are world readable. This can result in exposure of sensitive information (e.g., cleartext or encrypted datasource passwords).	5.5	More Details
CVE-2020-12459	In certain Red Hat packages for Grafana 6.x through 6.3.6, the configuration files /etc/grafana/grafana.ini and /etc/grafana/ldap.toml (which contain a secret_key and a bind_password) are world readable.	5.5	More Details
CVE-2020-5890	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1 and BIG-IQ 5.2.0-7.1.0, when creating a QKView, credentials for binding to LDAP servers used for remote authentication of the BIG-IP administrative interface will not fully obfuscate if they contain whitespace.	5.5	More Details
CVE-2018-21232	re2c before 2.0 has uncontrolled recursion that causes stack consumption in find_fixed_tags.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12656	gss_mech_free in net/sunrpc/auth_gss/gss_mech_switch.c in the rpcsec_gss_krb5 implementation in the Linux kernel through 5.6.10 lacks certain domain_release calls, leading to a memory leak. Note: This was disputed with the assertion that the issue does not grant any access not already available. It is a problem that on unloading a specific kernel module some memory is leaked, but loading kernel modules is a privileged operation. A user could also write a kernel module to consume any amount of memory they like and load that replicating the effect of this bug	5.5	More Details
CVE-2019-19102	A directory traversal vulnerability in SharpZipLib used in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x and 4.2.x allow unauthenticated users to write to certain local directories. The vulnerability is also known as zip slip.	5.5	More Details
CVE-2020-12655	An issue was discovered in xfs_agf_verify in fs/xfs/libxfs/xfs_alloc.c in the Linux kernel through 5.6.10. Attackers may trigger a sync of excessive duration via an XFS v5 image with crafted metadata, aka CID-d0c7feaf8767.	5.5	More Details
CVE-2019-12864	SolarWinds Orion Platform 2018.4 HF3 (NPM 12.4, NetPath 1.1.4) is vulnerable to Information Leakage, because of improper error handling with stack traces, as demonstrated by discovering a full pathname upon a 500 Internal Server Error via the api2/swis/query?lang=en-us&swAlertOnError=false query parameter.	5.5	More Details
CVE-2020-8472	Insufficient folder permissions used by system functions in ABB System 800xA products OPCServer for AC800M (versions 6.0 and earlier) and Control Builder M Professional, MMSServer for AC800M, Base Software for SoftControl (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploited the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	5.5	More Details
CVE-2020-10618	LCDS LAquis SCADA Versions 4.3.1 and prior. The affected product is vulnerable to sensitive information exposure by unauthorized users.	5.5	More Details
CVE-2020-6867	ZTE's SDON controller is impacted by the resource management error vulnerability. When RPC is frequently called by other applications in the case of mass traffic data in the system, it will result in no response for a long time and memory overflow risk. This affects: ZENIC ONE R22b versions V16.19.10P02SP002 and V16.19.10P02SP005.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12475	TP-Link Omada Controller Software 3.2.6 allows Directory Traversal for reading arbitrary files via com.tp_link.eap.web.portal.PortalController.getAdvertiseFile in /opt/tplink/EAPController/lib/eap-web-3.2.6.jar.	5.5	More Details
CVE-2019-19514	Ayision Ays-WR01 v28K.RPT.20161224 devices allow stored XSS in basic repeater settings via an SSID.	5.4	More Details
CVE-2020-12472	MonoX through 5.1.40.5152 allows stored XSS via User Status, Blog Comments, or Blog Description.	5.4	More Details
CVE-2020-5889	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, in BIG-IP APM portal access, a specially crafted HTTP request can lead to reflected XSS after the BIG-IP APM system rewrites the HTTP response from the untrusted backend server and sends it to the client.	5.4	More Details
CVE-2020-4209	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to create arbitrary files on the system. IBM X-Force ID: 175019.	5.4	More Details
CVE-2019-20768	ServiceNow IT Service Management Kingston through Patch 14-1, London through Patch 7, and Madrid before patch 4 allow stored XSS via crafted sysparm_item_guid and sys_id parameters in an Incident Request to service_catalog.do.	5.4	More Details
CVE-2019-7634	SUAP V2 allows XSS during the update of user information.	5.4	More Details
CVE-2020-12629	include/class.sla.php in osTicket before 1.14.2 allows XSS via the SLA Name.	5.4	More Details
CVE-2019-17557	It was found that the Apache Syncope EndUser UI login page prio to 2.0.15 and 2.1.6 reflects the successMessage parameters. By this mean, a user accessing the Enduser UI could execute javascript code from URL query string.	5.4	More Details
CVE-2020-10700	A use-after-free flaw was found in the way samba AD DC LDAP servers, handled 'Paged Results' control is combined with the 'ASQ' control. A malicious user in a samba AD could use this flaw to cause denial of service. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12277	GitLab 10.8 through 12.9 has a vulnerability that allows someone to mirror a repository even if the feature is not activated.	5.3	More Details
CVE-2020-8478	Insufficient protection of the inter-process communication functions in ABB System 800xA products OPC Server for AC 800M, MMS Server for AC 800M and Base Software for SoftControl (all published versions) enables an attacker authenticated on the local system to inject data, affecting the online view of runtime data shown in Control Builder.	5.3	More Details
CVE-2020-8476	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, ABB AbilityTM SCADAvantage versions 5.1 to 5.6.5, a weakness in validation of input exists that allows an attacker to alter licenses assigned to the system nodes by sending specially crafted messages to the CLS web service.	5.3	More Details
CVE-2020-12439	Grin before 3.1.0 allows attackers to adversely affect availability of data on a Mimblewimble blockchain.	5.3	More Details
CVE-2020-8792	The OKLOK (3.1.1) mobile companion app for Fingerprint Bluetooth Padlock FB50 (2.3) has an information-exposure issue. In the mobile app, an attempt to add an already-bound lock by its barcode reveals the email address of the account to which the lock is bound, as well as the name of the lock. Valid barcode inputs can be easily guessed because barcode strings follow a predictable pattern. Correctly guessed valid barcode inputs entered through the app interface disclose arbitrary users' email addresses and lock names.	5.3	More Details
CVE-2020-10933	An issue was discovered in Ruby 2.5.x through 2.5.7, 2.6.x through 2.6.5, and 2.7.0. If a victim calls BasicSocket#read_nonblock(requested_size, buffer, exception: false), the method resizes the buffer to fit the requested size, but no data is copied. Thus, the buffer string provides the previous value of the heap. This may expose possibly sensitive data from the interpreter.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12275	GitLab 12.6 through 12.9 is vulnerable to a privilege escalation that allows an external user to create a personal snippet through the API.	5.3	More Details
CVE-2020-8475	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, ABB AbilityTM SCADAvantage versions 5.1 to 5.6.5, a weakness in validation of input exists that allows an attacker to block license handling by sending specially crafted messages to the CLS web service.	5.3	More Details
CVE-2020-12117	Moxa Service in Moxa NPort 5150A firmware version 1.5 and earlier allows attackers to obtain sensitive configuration values via a crafted packet to UDP port 4800. NOTE: Moxa Service is an unauthenticated service that runs upon a first-time installation but can be disabled without ill effect.	5.3	More Details
CVE-2020-10691	An archive traversal flaw was found in all ansible-engine versions 2.9.x prior to 2.9.7, when running ansible-galaxy collection install. When extracting a collection .tar.gz file, the directory is created without sanitizing the filename. An attacker could take advantage to overwrite any file within the system.	5.2	More Details
CVE-2020-5335	RSA Archer, versions prior to 6.7 P2 (6.7.0.2), contain a cross-site request forgery vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to send arbitrary requests to the vulnerable application to perform server operations with the privileges of the authenticated victim user.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6866	A ZTE product is impacted by a resource management error vulnerability. An attacker could exploit this vulnerability to cause a denial of service by issuing a specific command. This affects: ZXCTN 6500 version V2.10.00R3B87.	4.9	More Details
CVE-2020-12142	1. IPSec UDP key material can be retrieved from machine-to-machine interfaces and human-accessible interfaces by a user with admin credentials. Such a user, with the required system knowledge, could use this material to decrypt in-flight communication. 2. The vulnerability requires administrative access and shell access to the EdgeConnect appliance. An admin user can access IPSec seed and nonce parameters using the CLI, REST APIs, and the Linux shell.	4.8	More Details
CVE-2020-12276	GitLab 9.5.9 through 12.9 is vulnerable to stored XSS in an admin notification feature.	4.8	More Details
CVE-2020-8799	A Stored XSS vulnerability has been found in the administration page of the WTI Like Post plugin through 1.4.5 for WordPress. Once the administrator has submitted the data, the script stored is executed for all the users visiting the website.	4.8	More Details
CVE-2020-12114	A pivot_root race condition in fs/namespace.c in the Linux kernel 4.4.x before 4.4.221, 4.9.x before 4.9.221, 4.14.x before 4.14.178, 4.19.x before 4.19.119, and 5.x before 5.3 allows local users to cause a denial of service (panic) by corrupting a mountpoint reference counter.	4.7	More Details
CVE-2020-5727	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to pair a rogue keypad to an armed system.	4.6	More Details
CVE-2020-5336	RSA Archer, versions prior to 6.7 P1 (6.7.0.1), contain a URL injection vulnerability. An unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to execute malicious JavaScript code on the affected system.	4.6	More Details
CVE-2020-5337	RSA Archer, versions prior to 6.7 P1 (6.7.0.1), contain a URL redirection vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to redirect application users to arbitrary web URLs by tricking the victim users to click on maliciously crafted links. The vulnerability could be used to conduct phishing attacks that cause users to unknowingly visit malicious sites.	4.6	More Details
CVE-2019-4288	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly senstiive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160631.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-4286	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly senstiive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160514.	4.3	More Details
CVE-2020-5333	RSA Archer, versions prior to 6.7 P3 (6.7.0.3), contain an authorization bypass vulnerability in the REST API. A remote authenticated malicious Archer user could potentially exploit this vulnerability to view unauthorized information.	4.3	More Details
CVE-2020-12101	The address-management feature in xt:Commerce 5.1 to 6.2.2 allows remote authenticated users to zero out other user's stored addresses by manipulating an id field in the POST request for altering an address.	4.3	More Details
CVE-2020-9387	In Mahara 19.04 before 19.04.5 and 19.10 before 19.10.3, account details are shared in the Elasticsearch results for accounts that are not accessible when the config setting 'Isolated institutions' is turned on.	4.3	More Details
CVE-2020-1732	A flaw was found in Soteria before 1.0.1, in a way that multiple requests occurring concurrently causing security identity corruption across concurrent threads when using EE Security with WildFly Elytron which can lead to the possibility of being handled using the identity from another request.	4.2	More Details
CVE-2020-8896	A Buffer Overflow vulnerability in the khcrypt implementation in Google Earth Pro versions up to and including 7.3.2 allows an attacker to perform a Man-in-the-Middle attack using a specially crafted key to read data past the end of the buffer used to hold it. Mitigation: Update to Google Earth Pro 7.3.3.	4.2	More Details
CVE-2020-12652	The __mptctl_ioctl function in drivers/message/fusion/mptctl.c in the Linux kernel before 5.4.14 allows local users to hold an incorrect lock during the ioctl operation and trigger a race condition, i.e., a "double fetch" vulnerability, aka CID-28d76df18f0a. NOTE: the vendor states "The security impact of this bug is not as bad as it could have been because these operations are all privileged and root already has enormous destructive power."	4.1	More Details
CVE-2020-10686	A flaw was found in Keycloak version 8.0.2 and 9.0.0, and was fixed in Keycloak version 9.0.1, where a malicious user registers as oneself. The attacker could then use the remove devices form to post different credential IDs and possibly remove MFA devices for other users.	4.1	More Details
CVE-2020-5893	In versions 7.1.5-7.1.8, when a user connects to a VPN using BIG-IP Edge Client over an unsecure network, BIG-IP Edge Client responds to authentication requests over HTTP while sending probes for captive portal detection.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10717	A potential DoS flaw was found in the virtio-fs shared file system daemon (virtiofsd) implementation of the QEMU version >= v5.0. Virtio-fs is meant to share a host file system directory with a guest via virtio-fs device. If the guest opens the maximum number of file descriptors under the shared directory, a denial of service may occur. This flaw allows a guest user/process to cause this denial of service on the host.	3.3	More Details
CVE-2020-12251	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an authenticated user to change the filename value (in the POST method) from the original filename to achieve directory traversal via a ../ sequence and, for example, obtain a complete directory listing of the machine.	2.2	More Details
CVE-2017-18771	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-20738, CVE-2017-18866. Reason: this candidate was intended for one issue, but the description and references inadvertently combined multiple issues. Notes: All CVE users should consult CVE-2019-20738 and CVE-2017-18866 to determine which ID is appropriate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2017-18774	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-21139, CVE-2017-18867. Reason: this candidate was intended for one issue, but the description and references inadvertently combined multiple issues. Notes: All CVE users should consult CVE-2018-21139 and CVE-2017-18867 to determine which ID is appropriate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2017-18760	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-20732, CVE-2017-18865. Reason: this candidate was intended for one issue, but the description and references inadvertently combined multiple issues. Notes: All CVE users should consult CVE-2019-20732 and CVE-2017-18865 to determine which ID is appropriate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-11495	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-2017-18753	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-20734, CVE-2017-18864. Reason: this candidate was intended for one issue, but the description and references inadvertently combined multiple issues. Notes: All CVE users should consult CVE-2019-20734 and CVE-2017-18864 to determine which ID is appropriate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details