SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 June 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-2020-11896	The Treck TCP/IP stack before 6.0.1.66 allows Remote Code Execution, related to IPv4 tunneling.	10.0	More Details
CVE-2020-11897	The Treck TCP/IP stack before 5.0.1.35 has an Out-of-Bounds Write via multiple malformed IPv6 packets.	10.0	More Details
CVE-2020-14993	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before 1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3663	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2020-14932	compose.php in SquirrelMail 1.4.22 calls unserialize for the $mailtodata value, which originates from an HTTP GET request. This is related to mailto.php.	9.8	More Details
CVE-2020-14942	Tendenci 12.0.10 allows unrestricted deserialization in apps\helpdesk\views\staff.py.	9.8	More Details
CVE-2019-14062	Buffer overflows while decoding setup message from Network due to lack of check of IE message length received from network in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SA415M, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14073	Copying RTCP messages into the output buffer without checking the destination buffer size which could lead to a remote stack overflow when processing large data or non-standard feedback messages in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, SA415M, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2019-14080	Out of bound write can happen due to lack of check of array index value while parsing SDP attribute for SAR in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS605, QM215, Rennell, SA415M, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2020-3614	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3628	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20	9.8	More Details
CVE-2020-3660	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2020-3661	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2020-3662	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2020-14967	An issue was discovered in the jsrsasign package before 8.0.18 for Node.js. Its RSA PKCS1 v1.5 decryption implementation does not detect ciphertext modification by prepending '\0' bytes to ciphertexts (it decrypts modified ciphertexts without error). An attacker might prepend these bytes with the goal of triggering memory corruption issues.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14938	An issue was discovered in map.c in FreedroidRPG 1.0rc2. It assumes lengths of data sets read from saved game files. It copies data from a file into a fixed-size heap-allocated buffer without size verification, leading to a heap-based buffer overflow.	9.8	More Details
CVE-2017-18920	An issue was discovered in Mattermost Server before 3.6.2. The WebSocket feature does not follow the Same Origin Policy.	9.8	More Details
CVE-2020-13159	Artica Proxy before 4.30.000000 Community Edition allows OS command injection via the Netbios name, Server domain name, dhclient_mac, Hostname, or Alias field. NOTE: this may overlap CVE-2020-10818.	9.8	More Details
CVE-2020-14972	Multiple SQL injection vulnerabilities in Sourcecodester Pisay Online E-Learning System 1.0 allow remote unauthenticated attackers to bypass authentication and achieve Remote Code Execution (RCE) via the user_email, user_pass, and id parameters on the admin login-portal and the edit-lessons webpages.	9.8	More Details
CVE-2020-11989	Apache Shiro before 1.5.3, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass.	9.8	More Details
CVE-2020-12053	In Unisys Stealth 3.4.x, 4.x and 5.x before 5.0.026, if certificate-based authorization is used without HTTPS, an endpoint could be authorized without a private key.	9.8	More Details
CVE-2020-14983	The server in Chocolate Doom 3.0.0 and Crispy Doom 5.8.0 doesn't validate the user-controlled num_players value, leading to a buffer overflow. A malicious user can overwrite the server's stack.	9.8	More Details
CVE-2020-14944	Global RADAR BSA Radar 1.6.7234.24750 and earlier lacks valid authorization controls in multiple functions. This can allow for manipulation and takeover of user accounts if successfully exploited. The following vulnerable functions are exposed: ChangePassword, SaveUserProfile, and GetUser.	9.8	More Details
CVE-2019-20409	The way in which velocity templates were used in Atlassian Jira Server and Data Center prior to version 8.8.0 allowed remote attackers to gain remote code execution if they were able to exploit a server side template injection vulnerability.	9.8	More Details
CVE-2020-12782	Openfind MailGates contains a Command Injection flaw, when receiving email with specific strings, malicious code in the mail attachment will be triggered and gain unauthorized access to system files.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5594	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors.	9.8	More Details
CVE-2020-14968	An issue was discovered in the jsrsasign package before 8.0.17 for Node.js. Its RSASSA-PSS (RSA-PSS) implementation does not detect signature manipulation/modification by prepending '\0' bytes to a signature (it accepts these modified signatures as valid). An attacker can abuse this behavior in an application by creating multiple valid signatures where only one signature should exist. Also, an attacker might prepend these bytes with the goal of triggering memory corruption issues.	9.8	More Details
CVE-2020-14931	A stack-based buffer overflow in DMitry (Deepmagic Information Gathering Tool) 1.3a might allow remote WHOIS servers to execute arbitrary code via a long line in a response that is mishandled by nic_format_buff.	9.8	More Details
CVE-2017-18915	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. After a restart of a server, an attacker might suddenly gain API Endpoint access.	9.8	More Details
CVE-2020-8165	A deserialization of untrusted data vulnernerability exists in rails < 5.2.4.3, rails < 6.0.3.1 that can allow an attacker to unmarshal user-provided objects in MemCacheStore and RedisCacheStore potentially resulting in an RCE.	9.8	More Details
CVE-2017-9109	An issue was discovered in adns before 1.5.2. It fails to ignore apparent answers before the first RR that was found the first time. when this is fixed, the second answer scan finds the same RRs at the first. Otherwise, adns can be confused by interleaving answers for the CNAME target, with the CNAME itself. In that case the answer data structure (on the heap) can be overrun. With this fixed, it prefers to look only at the answer RRs which come after the CNAME, which is at least arguably correct.	9.8	More Details
CVE-2017-9103	An issue was discovered in adns before 1.5.2. pap_mailbox822 does not properly check st from adns__findlabel_next. Without this, an uninitialised stack value can be used as the first label length. Depending on the circumstances, an attacker might be able to trick adns into crashing the calling program, leaking aspects of the contents of some of its memory, causing it to allocate lots of memory, or perhaps overrunning a buffer. This is only possible with applications which make non-raw queries for SOA or RP records.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-9104	An issue was discovered in adns before 1.5.2. It hangs, eating CPU, if a compression pointer loop is encountered.	9.8	More Details
CVE-2020-13640	A SQL injection issue in the gVectors wpDiscuz plugin 5.3.5 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the order parameter of a wpdLoadMoreComments request. (No 7.x versions are affected.)	9.8	More Details
CVE-2020-11503	A heap-based buffer overflow in the awarrensmtp component of Sophos XG Firewall v17.5 MR11 and older potentially allows an attacker to run arbitrary code remotely.	9.8	More Details
CVE-2017-18908	An issue was discovered in Mattermost Server before 4.0.0, 3.10.2, and 3.9.2. A password-reset request was sometime sent to an attacker-provided e-mail address.	9.8	More Details
CVE-2019-20856	An issue was discovered in Mattermost Desktop App before 4.3.0 on macOS. It allows dylib injection.	9.8	More Details
CVE-2018-21251	An issue was discovered in Mattermost Server before 5.2 and 5.1.1. Authorization could be bypassed if the channel name were not the same in the params and the body.	9.8	More Details
CVE-2019-20853	An issue was discovered in Mattermost Packages before 5.16.3. A Droplet could allow Internet access to a service that has a remote code execution problem.	9.8	More Details
CVE-2017-18900	An issue was discovered in Mattermost Server before 4.1.0, 4.0.4, and 3.10.3. It allows CSV injection via a compliance report.	9.8	More Details
CVE-2017-18885	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It allows attackers to gain privileges by accessing unintended API endpoints on a user's behalf.	9.8	More Details
CVE-2016-11074	An issue was discovered in Mattermost Server before 3.0.0. A password-reset link could be reused.	9.8	More Details
CVE-2016-11064	An issue was discovered in Mattermost Desktop App before 3.4.0. Strings could be executed as code via injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18912	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. It allows an attacker to specify a full pathname of a log file.	9.8	More Details
CVE-2020-9480	In Apache Spark 2.4.5 and earlier, a standalone resource manager's master may be configured to require authentication (spark.authenticate) via a shared secret. When enabled, however, a specially-crafted RPC to the master can succeed in starting an application's resources on the Spark cluster, even without the shared key. This can be leveraged to execute shell commands on the host machine. This does not affect Spark clusters using other resource managers (YARN, Mesos, etc).	9.8	More Details
CVE-2017-18888	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It allows SQL injection during the fetching of multiple posts.	9.8	More Details
CVE-2020-12884	A buffer over-read was discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse_multiple_options() parses CoAP options that may occur multiple consecutive times in a single packet. While processing the options, packet_data_pptr is accessed after being incremented by option_len without a prior out-of-bounds memory check. The temp_parsed_uri_query_ptr is validated for a correct range, but the range valid for temp_parsed_uri_query_ptr is derived from the amount of allocated heap memory, not the actual input size. Therefore the check of temp_parsed_uri_query_ptr may be insufficient for safe access to the area pointed to by packet_data_pptr. As a result, access to a memory area outside of the intended boundary of the packet buffer is made.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12883	Buffer over-reads were discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses CoAP input linearly using a while loop. Once an option is parsed in a loop, the current point (*packet_data_pptr) is increased correspondingly. The pointer is restricted by the size of the received buffer, as well as by the option delta and option length bytes. The actual input packet length is not verified against the number of bytes read when processing the option extended delta and the option extended length. Moreover, the calculation of the message_left variable, in the case of non-extended option deltas, is incorrect and indicates more data left for processing than provided in the function input. All of these lead to heap-based or stack-based memory location read access that is outside of the intended boundary of the buffer. Depending on the platform-specific memory management mechanisms, it can lead to processing of unintended inputs or system memory access violation errors.	9.1	More Details
CVE-2020-12886	A buffer over-read was discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses the CoAP packet header starting from the message token. The length of the token in the received message is provided in the first byte parsed by the sn_coap_parser_options_parse() function. The length encoded in the message is not validated against the actual input buffer length before accessing the token. As a result, memory access outside of the intended boundary of the buffer may occur.	9.1	More Details
CVE-2017-18911	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. The X.509 certificate validation can be skipped for a TLS-based e-mail server.	9.1	More Details
CVE-2019-20851	An issue was discovered in Mattermost Mobile Apps before 1.26.0. An attacker can use directory traversal with the Video Preview feature to overwrite arbitrary files on a device.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3658	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.1	More Details
CVE-2020-11898	The Treck TCP/IP stack before 6.0.1.66 improperly handles an IPv4/ICMPv4 Length Parameter Inconsistency, which might allow remote attackers to trigger an information leak.	9.1	More Details
CVE-2017-18883	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2, when serving as an OAuth 2.0 Service Provider. There is low entropy for authorization data.	9.1	More Details
CVE-2020-11901	The Treck TCP/IP stack before 6.0.1.66 allows Remote Code execution via a single invalid DNS response.	9.0	More Details
CVE-2020-12021	In OSIsoft PI Web API 2019 Patch 1 (1.12.0.6346) and all previous versions, the affected product is vulnerable to a cross-site scripting attack, which may allow an attacker to remotely execute arbitrary code.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-12033	In Rockwell Automation FactoryTalk Services Platform, all versions, the redundancy host service (RdcyHost.exe) does not validate supplied identifiers, which could allow an unauthenticated, adjacent attacker to execute remote COM objects with elevated privileges.	8.8	More Details
CVE-2019-20861	An issue was discovered in Mattermost Desktop App before 4.2.2. It allows attackers to execute arbitrary code via a crafted link.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18886	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It allows a bypass of restrictions on use of slash commands.	8.8	More Details
CVE-2020-14426	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11.	8.8	More Details
CVE-2017-9105	An issue was discovered in adns before 1.5.2. It corrupts a pointer when a nameserver speaks first because of a wrong number of pointer dereferences. This bug may well be exploitable as a remote code execution.	8.8	More Details
CVE-2018-21264	An issue was discovered in Mattermost Server before 4.7.0, 4.6.2, and 4.5.2. It did not enforce the expiration date of a SAML response.	8.8	More Details
CVE-2020-14933	compose.php in SquirrelMail 1.4.22 calls unserialize for the $attachments value, which originates from an HTTP POST request. NOTE: the vendor disputes this because these two conditions for PHP object injection are not satisfied: existence of a PHP magic method (such as __wakeup or __destruct), and any attack-relevant classes must be declared before unserialize is called (or must be autoloaded).	8.8	More Details
CVE-2020-14950	aaPanel through 6.6.6 allows remote authenticated users to execute arbitrary commands via shell metacharacters in a modified /system?action=ServiceAdmin request (start, stop, or restart) to the setting menu of Sotfware Store.	8.8	More Details
CVE-2019-20865	An issue was discovered in Mattermost Server before 5.12.0, 5.11.1, 5.10.2, 5.9.2, and 4.10.10. The login page allows CSRF.	8.8	More Details
CVE-2020-14429	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3342	A vulnerability in the software update feature of Cisco Webex Meetings Desktop App for Mac could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. The vulnerability is due to improper validation of cryptographic protections on files that are downloaded by the application as part of a software update. An attacker could exploit this vulnerability by persuading a user to go to a website that returns files to the client that are similar to files that are returned from a valid Webex website. The client may fail to properly validate the cryptographic protections of the provided files before executing them as part of an update. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the user.	8.8	More Details
CVE-2020-13155	clearsystem.php in NukeViet 4.4 allows CSRF with resultant HTML injection via the deltype parameter to the admin/index.php?nv=webtools&op=clearsystem URI.	8.8	More Details
CVE-2020-13887	documents_add.php in Kordil EDMS through 2.2.60rc3 allows Remote Command Execution because .php files can be uploaded to the documents folder.	8.8	More Details
CVE-2020-14203	WebFOCUS Business Intelligence 8.0 (SP6) allows a Cross-Site Request Forgery (CSRF) attack against administrative users within the /ibi_apps/WFServlet(.ibfs) endpoint. The impact may be creation of an administrative user. It can also be exploited in conjunction with CVE-2016-9044.	8.8	More Details
CVE-2020-8102	Improper Input Validation vulnerability in the Safepay browser component of Bitdefender Total Security 2020 allows an external, specially crafted web page to run remote commands inside the Safepay Utility process. This issue affects Bitdefender Total Security 2020 versions prior to 24.0.20.116.	8.8	More Details
CVE-2018-21263	An issue was discovered in Mattermost Server before 4.7.0, 4.6.2, and 4.5.2. An attacker could authenticate to a different user's account via a crafted SAML response.	8.8	More Details
CVE-2020-14427	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14428	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14430	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2017-18903	An issue was discovered in Mattermost Server before 4.0.0, 3.10.2, and 3.9.2. CSRF can occur if CORS is enabled.	8.8	More Details
CVE-2019-20841	An issue was discovered in Mattermost Server before 5.18.0, 5.17.2, 5.16.4, 5.15.4, and 5.9.7. CSRF can sometimes occur via a crafted web site for account takeover attacks.	8.8	More Details
CVE-2020-14443	A SQL injection vulnerability in accountancy/customer/card.php in Dolibarr 11.0.3 allows remote authenticated users to execute arbitrary SQL commands via the id parameter.	8.8	More Details
CVE-2020-14442	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14441	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14440	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14439	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14438	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14437	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14436	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	8.8	More Details
CVE-2019-20891	WooCommerce before 3.6.5, when it handles CSV imports of products, has a cross-site request forgery (CSRF) issue with resultant stored cross-site scripting (XSS) via includes/admin/importers/class-wc-product-csv-importer-controller.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14435	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104.	8.8	More Details
CVE-2020-14432	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-13224	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow	8.8	More Details
CVE-2020-14431	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	8.8	More Details
CVE-2020-14945	A privilege escalation vulnerability exists within Global RADAR BSA Radar 1.6.7234.24750 and earlier that allows an authenticated, low-privileged user to escalate their privileges to administrator rights (i.e., the BankAdmin role) via modified SaveUser data.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4062	In Conjur OSS Helm Chart before 2.0.0, a recently identified critical vulnerability resulted in the installation of the Conjur Postgres database with an open port. This allows an attacker to gain full read & write access to the Conjur Postgres database, including escalating the attacker's privileges to assume full control. A malicious actor who knows the IP address and port number of the Postgres database and has access into the Kubernetes cluster where Conjur runs can gain full read & write access to the Postgres database. This enables the attacker to write a policy that allows full access to retrieve any secret. This Helm chart is a method to install Conjur OSS into a Kubernetes environment. Hence, the systems impacted are only Conjur OSS systems that were deployed using this chart. Other deployments including Docker and the CyberArk Dynamic Access Provider (DAP) are not affected. To remediate this vulnerability, clone the latest Helm Chart and follow the upgrade instructions. If you are not able to fully remediate this vulnerability immediately, you can mitigate some of the risk by making sure Conjur OSS is deployed on an isolated Kubernetes cluster or namespace. The term "isolated" refers to: - No other workloads besides Conjur OSS and its backend database are running in that Kubernetes cluster/namespace. - Kubernetes and helm access to the cluster/namespace is limited to security administrators via Role-Based Access Control (RBAC).	8.7	More Details
CVE-2020-13279	Client side code execution in gitlab-vscode-extension v2.2.0 allows attacker to execute code on user system	8.6	More Details
CVE-2020-14461	Zyxel Armor X1 WAP6806 1.00(ABAL.6)C0 devices allow Directory Traversal via the images/eaZy/ URI.	8.6	More Details
CVE-2020-11900	The Treck TCP/IP stack before 6.0.1.41 has an IPv4 tunneling Double Free.	8.2	More Details
CVE-2020-14204	In WebFOCUS Business Intelligence 8.0 (SP6), the administration portal allows remote attackers to read arbitrary local files or forge server-side HTTP requests via a crafted HTTP request to /ibi_apps/WFServlet.cfg because XML external entity injection is possible. This is related to making changes to the application repository configuration.	8.2	More Details
CVE-2020-6869	All versions up to 10.06 of ZTEMarket APK are impacted by an information leak vulnerability. Due to Activity Component exposure users can exploit this vulnerability to get the private cookie and execute silent installation.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14977	An issue was discovered in F-Secure SAFE 17.7 on macOS. The XPC services use the PID to identify the connecting client, which allows an attacker to perform a PID reuse attack and connect to a privileged XPC service, and execute privileged commands on the system. NOTE: the attacker needs to execute code on an already compromised machine.	8.1	More Details
CVE-2020-5590	Directory traversal vulnerability in EC-CUBE 3.0.0 to 3.0.18 and 4.0.0 to 4.0.3 allows remote authenticated attackers to delete arbitrary files and/or directories on the server via unspecified vectors.	8.1	More Details
CVE-2020-3361	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to gain unauthorized access to a vulnerable Webex site. The vulnerability is due to improper handling of authentication tokens by a vulnerable Webex site. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Cisco Webex Meetings Server site. If successful, the attacker could gain the privileges of another user within the affected Webex site.	8.1	More Details
CVE-2020-6644	An insufficient session expiration vulnerability in FortiDeceptor 3.0.0 and below allows an attacker to reuse the unexpired admin user session IDs to gain admin privileges, should the attacker be able to obtain that session ID via other, hypothetical attacks.	8.1	More Details
CVE-2017-18884	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It allows attackers to gain privileges by using a registered OAuth application with personal access tokens.	8.1	More Details
CVE-2017-18894	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5, when used as an OAuth 2.0 service provider. Sometimes. resource-owner authorization is bypassed, allowing account takeover.	8.1	More Details
CVE-2020-14930	An issue was discovered in BT CTROMS Terminal OS Port Portal CT-464. Account takeover can occur because the password-reset feature discloses the verification token. Upon a getverificationcode.jsp request, this token is transmitted not only to the registered phone number of the user account, but is also transmitted to the unauthenticated HTTP client.	8.1	More Details
CVE-2020-14978	An issue was discovered in F-Secure SAFE 17.7 on macOS. Due to incorrect client version verification, an attacker can connect to a privileged XPC service, and execute privileged commands on the system. NOTE: the attacker needs to execute code on an already compromised machine.	8.1	More Details
CVE-2017-18906	An issue was discovered in Mattermost Server before 4.0.0, 3.10.2, and 3.9.2, when Single Sign-On OAuth2 is used. An attacker could claim somebody else's account.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14157	The wireless-communication feature of the ABUS Secvest FUBE50001 device does not encrypt sensitive data such as PIN codes or IDs of used proximity chip keys (RFID tokens). This makes it easier for an attacker to disarm the wireless alarm system.	8.1	More Details
CVE-2019-14894	A flaw was found in the CloudForms management engine version 5.10 and CloudForms management version 5.11, which triggered remote code execution through NFS schedule backup. An attacker logged into the management console could use this flaw to execute arbitrary shell commands on the CloudForms server as root.	8.0	More Details
CVE-2020-13275	A user with an unverified email address could request an access to domain restricted groups in GitLab EE 12.2 and later through 13.0.1	8.0	More Details
CVE-2020-10736	An authorization bypass vulnerability was found in Ceph versions 15.2.0 before 15.2.2, where the ceph-mon and ceph-mgr daemons do not properly restrict access, resulting in gaining access to unauthorized resources. This flaw allows an authenticated client to modify the configuration and possibly conduct further attacks.	8.0	More Details
CVE-2020-14975	The driver in IOBit Unlocker 1.1.2 allows a low-privileged user to delete, move, or copy arbitrary files via IOCTL code 0x222124.	7.8	More Details
CVE-2020-8903	A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to escalate privileges to root. Using their membership to the "adm" group, users with this role are able to read the DHCP XID from the systemd journal. Using the DHCP XID, it is then possible to set the IP address and hostname of the instance to any value, which is then stored in /etc/hosts. An attacker can then point metadata.google.internal to an arbitrary IP address and impersonate the GCE metadata server which make it is possible to instruct the OS Login PAM module to grant administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "adm" user from the OS Login entry.	7.8	More Details
CVE-2020-9225	FusionSphere OpenStack 6.5.1 have an improper permissions management vulnerability. The software does not correctly perform a privilege assignment when an actor attempts to perform an action. Successful exploit could allow certain user to do certain operations beyond its privilege.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11520	The SDDisk2k.sys driver of WinMagic SecureDoc v8.5 and earlier allows local users to write to arbitrary kernel memory addresses because the IOCTL dispatcher lacks pointer validation. Exploiting this vulnerability results in privileged code execution.	7.8	More Details
CVE-2019-14094	Integer overflow in diag command handler when user inputs a large value for number of tasks field in the request packet in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096AU, APQ8098, IPQ6018, IPQ8074, Kamorta, MDM9150, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCM2150, QCN7605, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-11519	The SDDisk2k.sys driver of WinMagic SecureDoc v8.5 and earlier allows local users to read or write to physical disc sectors via a \\.\SecureDocDevice handle. Exploiting this vulnerability results in privileged code execution.	7.8	More Details
CVE-2019-10597	kernel writes to user passed address without any checks can lead to arbitrary memory write in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, MSM8996, MSM8996AU, Nicobar, QCS605, Rennell, Saipan, SC7180, SC8180X, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-8933	A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to escalate privileges to root. Using the membership to the "lxd" group, an attacker can attach host devices and filesystems. Within an lxc container, it is possible to attach the host OS filesystem and modify /etc/sudoers to then gain administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "lxd" user from the OS Login entry.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8907	A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to escalate privileges to root. Using their membership to the "docker" group, an attacker with this role is able to run docker and mount the host OS. Within docker, it is possible to modify the host OS filesystem and modify /etc/groups to gain administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "docker" user from the OS Login entry.	7.8	More Details
CVE-2020-14019	Open-iSCSI rtslib-fb through 2.1.72 has weak permissions for /etc/target/saveconfig.json because shutil.copyfile (instead of shutil.copy) is used, and thus permissions are not preserved.	7.8	More Details
CVE-2020-14939	An issue was discovered in savestruct_internal.c in FreedroidRPG 1.0rc2. Saved game files are composed of Lua scripts that recover a game's state. A file can be modified to put any Lua code inside, leading to arbitrary code execution while loading.	7.8	More Details
CVE-2020-3613	Double free issue in kernel memory mapping due to lack of memory protection mechanism in Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in SM8150	7.8	More Details
CVE-2020-3676	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-3665	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14971	Pi-hole through 5.0 allows code injection in piholedhcp (the Static DHCP Leases section) by modifying Teleporter backup files and then restoring them. This occurs in settings.php. To exploit this, an attacker would request a backup of limited files via teleporter.php. These are placed into a .tar.gz archive. The attacker then modifies the host parameter in dnsmasq.d files, and then compresses and uploads these files again.	7.8	More Details
CVE-2020-3635	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14076	Buffer overflow occurs while processing an subsample data length out of range due to lack of user input validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14047	While IPA driver processes route add rule IOCTL, there is no input validation of the rule ID prior to adding the rule to the IPA HW commit list in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8096AU, MDM9607, MSM8909W, MSM8996, MSM8996AU, QCN7605, QCS605, SC8180X, SDA845, SDX20, SDX24, SDX55, SM8150, SXR1130	7.8	More Details
CVE-2020-9332	ftusbbus2.sys in FabulaTech USB for Remote Desktop through 2020-02-19 allows privilege escalation via crafted IoCtl code related to a USB HID device.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3642	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-3626	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2019-14091	Double free issue in NPU due to lack of resource locking mechanism to avoid race condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, QCS405, Rennell, Saipan, SC8180X, SDX55, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-14447	An issue was discovered in Mattermost Server before 5.23.0. Large webhook requests allow attackers to cause a denial of service (infinite loop), aka MMSA-2020-0021.	7.5	More Details
CVE-2017-18871	An issue was discovered in Mattermost Server before 4.5.0, 4.4.5, 4.3.4, and 4.2.2. It allows attackers to cause a denial of service (application crash) via an @ character before a JavaScript field name.	7.5	More Details
CVE-2018-21262	An issue was discovered in Mattermost Server before 4.7.3. It allows attackers to cause a denial of service (application crash) via invalid LaTeX text.	7.5	More Details
CVE-2020-13272	OAuth flow missing verification checks CE/EE 12.3 and later through 13.0.1 allows unverified user to use OAuth authorization code flow	7.5	More Details
CVE-2020-13274	A security issue allowed achieving Denial of Service attacks through memory exhaustion by uploading malicious artifacts in all previous GitLab versions through 13.0.1	7.5	More Details
CVE-2020-13273	A Denial of Service vulnerability allowed exhausting the system resources in GitLab CE/EE 12.0 and later through 13.0.1	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18909	An issue was discovered in Mattermost Server before 3.9.0 when SAML is used. Encryption and signature verification are not mandatory.	7.5	More Details
CVE-2020-14448	An issue was discovered in Mattermost Server before 5.23.0. Automatic direct message replies allow attackers to cause a denial of service (infinite loop), aka MMSA-2020-0020.	7.5	More Details
CVE-2017-18917	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. Weak hashing was used for e-mail invitations, OAuth, and e-mail verification tokens.	7.5	More Details
CVE-2020-14929	Alpine before 2.23 silently proceeds to use an insecure connection after a /tls is sent in certain circumstances involving PREAUTH, which is a less secure behavior than the alternative of closing the connection and letting the user decide what they would like to do.	7.5	More Details
CVE-2015-9548	An issue was discovered in Mattermost Server before 1.2.0. It allows attackers to cause a denial of service (memory consumption) via a small compressed file that has a large size when uncompressed.	7.5	More Details
CVE-2019-20880	An issue was discovered in Mattermost Server before 5.8.0, 5.7.2, 5.6.5, and 4.10.7. It allows attackers to cause a denial of service (memory consumption) via OpenGraph.	7.5	More Details
CVE-2019-20846	An issue was discovered in Mattermost Server before 5.18.0. It has weak permissions for server-local file storage.	7.5	More Details
CVE-2016-11066	An issue was discovered in Mattermost Server before 3.2.0. The initial_load API disclosed unnecessary personal information.	7.5	More Details
CVE-2019-20845	An issue was discovered in Mattermost Server before 5.18.0. It allows attackers to cause a denial of service (memory consumption) via a large Slack import.	7.5	More Details
CVE-2019-20843	An issue was discovered in Mattermost Server before 5.18.0, 5.17.2, 5.16.4, 5.15.4, and 5.9.7. There are weak permissions for configuration files.	7.5	More Details
CVE-2016-11069	An issue was discovered in Mattermost Server before 3.2.0. It mishandles brute-force attempts at password change.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21258	An issue was discovered in Mattermost Server before 5.1. It allows attackers to cause a denial of service via the invite_people slash command.	7.5	More Details
CVE-2020-14449	An issue was discovered in Mattermost Mobile Apps before 1.30.0. Authorization tokens can sometimes be disclosed to third-party servers, aka MMSA-2020-0018.	7.5	More Details
CVE-2019-20885	An issue was discovered in Mattermost Server before 5.8.0. It does not always generate a robots.txt file.	7.5	More Details
CVE-2020-8184	A reliance on cookies without validation/integrity check security vulnerability exists in rack < 2.2.3, rack < 2.1.4 that makes it is possible for an attacker to forge a secure or host-only cookie prefix.	7.5	More Details
CVE-2018-21248	An issue was discovered in Mattermost Server before 5.4.0. It mishandles possession of superfluous authentication credentials.	7.5	More Details
CVE-2019-20874	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. It allows attackers to obtain sensitive information during a role change.	7.5	More Details
CVE-2019-20871	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. The Markdown library allows catastrophic backtracking.	7.5	More Details
CVE-2019-20886	An issue was discovered in Mattermost Server before 5.8.0. The first user is sometimes inadvertently a system admin.	7.5	More Details
CVE-2019-20888	An issue was discovered in Mattermost Server before 5.7, 5.6.3, 5.5.2, and 4.10.5. It allows attackers to cause a denial of service (memory consumption) via an outgoing webhook or a slash command integration.	7.5	More Details
CVE-2019-20868	An issue was discovered in Mattermost Server before 5.11.0. Invite IDs were improperly generated.	7.5	More Details
CVE-2020-8162	A client side enforcement of server side security vulnerability exists in rails < 5.2.4.2 and rails < 6.0.3.1 ActiveStorage's S3 adapter that allows the Content-Length of a direct file upload to be modified by an end user bypassing upload limits.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8164	A deserialization of untrusted data vulnerability exists in rails < 5.2.4.3, rails < 6.0.3.1 which can allow an attacker to supply information can be inadvertently leaked fromStrong Parameters.	7.5	More Details
CVE-2019-20864	An issue was discovered in Mattermost Plugins before 5.13.0. The GitHub plugin allows an attacker to attach his Mattermost account to a different person's GitHub account.	7.5	More Details
CVE-2019-20863	An issue was discovered in Mattermost Server before 5.13.0. Incoming webhook creation is not properly restricted.	7.5	More Details
CVE-2019-20862	An issue was discovered in Mattermost Server before 5.13.0. Non-members may fetch a team's slash commands.	7.5	More Details
CVE-2019-20859	An issue was discovered in Mattermost Server before 5.15.0. Login access control can be bypassed via crafted input.	7.5	More Details
CVE-2020-14450	An issue was discovered in Mattermost Server before 5.22.0. The markdown renderer allows attackers to cause a denial of service (client-side), aka MMSA-2020-0017.	7.5	More Details
CVE-2020-14969	app/Model/Attribute.php in MISP 2.4.127 lacks an ACL lookup on attribute correlations. This occurs when querying the attribute restsearch API, revealing metadata about a correlating but unreachable attribute.	7.5	More Details
CVE-2020-14966	An issue was discovered in the jsrsasign package through 8.0.18 for Node.js. It allows a malleability in ECDSA signatures by not checking overflows in the length of a sequence and '0' characters appended or prepended to an integer. The modified signatures are verified as valid. This could have a security-relevant impact if an application relied on a single canonical signature.	7.5	More Details
CVE-2019-20857	An issue was discovered in Mattermost Server before 5.16.0. It allows attackers to cause a denial of service (markdown renderer hang) via many backtick characters.	7.5	More Details
CVE-2019-20855	An issue was discovered in Mattermost Server before 5.16.1, 5.15.2, 5.14.5, and 5.9.6. It allows attackers to obtain sensitive information (local files) during legacy attachment migration.	7.5	More Details
CVE-2019-20854	An issue was discovered in Mattermost Server before 5.17.0. It allows remote attackers to cause a denial of service (client-side application crash) via a LaTeX message.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20852	An issue was discovered in Mattermost Mobile Apps before 1.26.0. Local logging is not blocked for sensitive information (e.g., server addresses or message content).	7.5	More Details
CVE-2020-14459	An issue was discovered in Mattermost Server before 5.19.0. Attackers can rename a channel and cause a collision with a direct message, aka MMSA-2020-0002.	7.5	More Details
CVE-2020-13263	An authorization issue relating to project maintainer impersonation was identified in GitLab EE 9.5 and later through 13.0.1 that could allow unauthorized users to impersonate as a maintainer to perform limited actions.	7.5	More Details
CVE-2020-14458	An issue was discovered in Mattermost Server before 5.19.0. Attackers can discover private channels via the "get channel by name" API, aka MMSA-2020-0004.	7.5	More Details
CVE-2020-14453	An issue was discovered in Mattermost Server before 5.21.0. Socket read operations are not appropriately restricted, which allows attackers to cause a denial of service, aka MMSA-2020-0005.	7.5	More Details
CVE-2020-14451	An issue was discovered in Mattermost Mobile Apps before 1.29.0. The iOS app allowed Single Sign-On cookies and Local Storage to remain after a logout, aka MMSA-2020-0013.	7.5	More Details
CVE-2019-20858	An issue was discovered in Mattermost Server before 5.15.0. It allows attackers to cause a denial of service (CPU consumption) via crafted characters in a SQL LIKE clause to an APIv4 endpoint.	7.5	More Details
CVE-2019-20848	An issue was discovered in Mattermost Mobile Apps before 1.26.0. The Quick Reply feature mishandles crafted replies.	7.5	More Details
CVE-2020-7668	In all versions of the package github.com/unknwon/cae/tz, the ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide.	7.5	More Details
CVE-2020-14399	An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint32_t pointers in libvncclient/rfbproto.c. NOTE: there is reportedly "no trust boundary crossed.	7.5	More Details
CVE-2020-14397	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rfbregion.c has a NULL pointer dereference.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14400	An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint16_t pointers in libvncserver/translate.c. NOTE: Third parties do not consider this to be a vulnerability as there is no known path of exploitation or cross of a trust boundary	7.5	More Details
CVE-2017-9106	An issue was discovered in adns before 1.5.2. adns_rr_info mishandles a bogus *datap. The general pattern for formatting integers is to sprintf into a fixed-size buffer. This is correct if the input is in the right range; if it isn't, the buffer may be overrun (depending on the sizes of the types on the current platform). Of course the inputs ought to be right. And there are pointers in there too, so perhaps one could say that the caller ought to check these things. It may be better to require the caller to make the pointer structure right, but to have the code here be defensive about (and tolerate with an error but without crashing) out-of-range integer values. So: it should defend each of these integer conversion sites with a check for the actual permitted range, and return adns_s_invaliddata if not. The lack of this check causes the SOA sign extension bug to be a serious security problem: the sign extended SOA value is out of range, and overruns the buffer when reconverted. This is related to sign extending SOA 32-bit integer fields, and use of a signed data type.	7.5	More Details
CVE-2017-9107	An issue was discovered in adns before 1.5.2. It overruns reading a buffer if a domain ends with backslash. If the query domain ended with \, and adns_qf_quoteok_query was specified, qdparselabel would read additional bytes from the buffer and try to treat them as the escape sequence. It would depart the input buffer and start processing many bytes of arbitrary heap data as if it were the query domain. Eventually it would run out of input or find some other kind of error, and declare the query domain invalid. But before then it might outrun available memory and crash. In principle this could be a denial of service attack.	7.5	More Details
CVE-2020-3263	A vulnerability in Cisco Webex Meetings Desktop App could allow an unauthenticated, remote attacker to execute programs on an affected end-user system. The vulnerability is due to improper validation of input that is supplied to application URLs. The attacker could exploit this vulnerability by persuading a user to follow a malicious URL. A successful exploit could allow the attacker to cause the application to execute other programs that are already present on the end-user system. If malicious files are planted on the system or on an accessible network file path, the attacker could execute arbitrary code on the affected system.	7.5	More Details
CVE-2020-14396	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-9108	An issue was discovered in adns before 1.5.2. adnshost mishandles a missing final newline on a stdin read. It is wrong to increment used as well as setting r, since used is incremented according to r, later. Rather one should be doing what read() would have done. Without this fix, adnshost may read and process one byte beyond the buffer, perhaps crashing or perhaps somehow leaking the value of that byte.	7.5	More Details
CVE-2019-20840	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/ws_decode.c can lead to a crash because of unaligned accesses in hybiReadAndDecode.	7.5	More Details
CVE-2019-20839	libvncclient/sockets.c in LibVNCServer before 0.9.13 has a buffer overflow via a long socket filename.	7.5	More Details
CVE-2020-14049	Viber for Windows up to 13.2.0.39 does not properly quote its custom URI handler. A malicious website could launch Viber with arbitrary parameters, forcing a victim to send an NTLM authentication request, and either relay the request or capture the hash for offline password cracking. NOTE: this issue exists because of an incomplete fix for CVE-2019-12569.	7.5	More Details
CVE-2018-21247	An issue was discovered in LibVNCServer before 0.9.13. There is an information leak (of uninitialized memory contents) in the libvncclient/rfbproto.c ConnectToRFBRepeater function.	7.5	More Details
CVE-2020-14398	An issue was discovered in LibVNCServer before 0.9.13. An improperly closed TCP connection causes an infinite loop in libvncclient/sockets.c.	7.5	More Details
CVE-2019-9943	In ome.services.graphs.GraphTraversal.findObjectDetails in Open Microscopy Environment OMERO.server 5.1.0 through 5.6.0, permissions on OMERO model objects may be circumvented during certain operations such as move and delete, because group permissions are mishandled.	7.5	More Details
CVE-2019-9944	In Open Microscopy Environment OMERO.server 5.0.0 through 5.6.0, the reading of files from imported image filesets may circumvent OMERO permissions restrictions. This occurs because the Bio-Formats feature allows an image file to have embedded pathnames.	7.5	More Details
CVE-2020-13637	An issue was discovered in the stashcat app through 3.9.2 for macOS, Windows, Android, iOS, and possibly other platforms. It stores the client_key, the device_id, and the public key for end-to-end encryption in cleartext, enabling an attacker (by copying or having access to the local storage database file) to login to the system from any other computer, and get unlimited access to all data in the users's context.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7664	In all versions of the package github.com/unknwon/cae/zip, the ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide.	7.5	More Details
CVE-2020-13158	Artica Proxy before 4.30.000000 Community Edition allows Directory Traversal via the fw.progrss.details.php popup parameter.	7.5	More Details
CVE-2020-14040	The x/text package before 0.3.3 for Go has a vulnerability in encoding/unicode that could lead to the UTF-16 decoder entering an infinite loop, causing the program to crash or run out of memory. An attacker could provide a single byte to a UTF16 decoder instantiated with UseBOM or ExpectBOM to trigger an infinite loop if the String function on the Decoder is called, or the Decoder is passed to golang.org/x/text/transform.String.	7.5	More Details
CVE-2020-14940	An issue was discovered in io/gpx/GPXDocumentReader.java in TuxGuitar 1.5.4. It uses misconfigured XML parsers, leading to XXE while loading GP6 (.gpx) and GP7 (.gp) tablature files.	7.5	More Details
CVE-2020-12885	An infinite loop was discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse_multiple_options() parses CoAP options in a while loop. This loop's exit condition is computed using the previously allocated heap memory required for storing the result of parsing multiple options. If the input heap memory calculation results in zero bytes, the loop exit condition is never met and the loop is not terminated. As a result, the packet parsing function never exits, leading to resource consumption.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12887	Memory leaks were discovered in the CoAP library in Arm Mbed OS 5.15.3 when using the Arm mbed-coap library 5.1.5. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses the CoAP option number field of all options present in the input packet. Each option number is calculated as a sum of the previous option number and a delta of the current option. The delta and the previous option number are expressed as unsigned 16-bit integers. Due to lack of overflow detection, it is possible to craft a packet that wraps the option number around and results in the same option number being processed again in a single packet. Certain options allocate memory by calling a memory allocation function. In the cases of COAP_OPTION_URI_QUERY, COAP_OPTION_URI_PATH, COAP_OPTION_LOCATION_QUERY, and COAP_OPTION_ETAG, there is no check on whether memory has already been allocated, which in conjunction with the option number integer overflow may lead to multiple assignments of allocated memory to a single pointer. This has been demonstrated to lead to memory leak by buffer orphaning. As a result, the memory is never freed.	7.5	More Details
CVE-2020-5367	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit.	7.4	More Details
CVE-2020-13276	User is allowed to set an email as a notification email even without verifying the new email in all previous GitLab CE/EE versions through 13.0.1	7.4	More Details
CVE-2019-20881	An issue was discovered in Mattermost Server before 5.8.0. It mishandles brute-force attacks against MFA.	7.3	More Details
CVE-2020-7679	In all versions of package casperjs, the mergeObjects utility function is susceptible to Prototype Pollution.	7.3	More Details
CVE-2020-4059	In mversion before 2.0.0, there is a command injection vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This vulnerability is patched by version 2.0.0. Previous releases are deprecated in npm. As a workaround, make sure to escape git commit messages when using the commitMessage option for the update function.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14456	An issue was discovered in Mattermost Desktop App before 4.4.0. The Same Origin Policy is mishandled during access-control decisions for web APIs, aka MMSA-2020-0006.	7.3	More Details
CVE-2020-11904	The Treck TCP/IP stack before 6.0.1.66 has an Integer Overflow during Memory Allocation that causes an Out-of-Bounds Write.	7.3	More Details
CVE-2020-11902	The Treck TCP/IP stack before 6.0.1.66 has an IPv6OverIPv4 tunneling Out-of-bounds Read.	7.3	More Details
CVE-2020-3290	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3291	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3289	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3288	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3287	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3275	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3286	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3292	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3279	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3276	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3274	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3269	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3293	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3268	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory.	7.2	More Details
CVE-2020-14960	A SQL injection vulnerability in PHP-Fusion 9.03.50 affects the endpoint administration/comments.php via the ctype parameter,	7.2	More Details
CVE-2020-3294	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3295	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3296	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-3336	A vulnerability in the software upgrade process of Cisco TelePresence Collaboration Endpoint Software and Cisco RoomOS Software could allow an authenticated, remote attacker to modify the filesystem to cause a denial of service (DoS) or gain privileged access to the root filesystem. The vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending requests with malformed parameters to the system using the console, Secure Shell (SSH), or web API. A successful exploit could allow the attacker to modify the device configuration or cause a DoS.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3278	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-14421	aaPanel through 6.6.6 allows remote authenticated users to execute arbitrary commands via the Script Content box on the Add Cron Job screen.	7.2	More Details
CVE-2020-14295	A SQL injection issue in color.php in Cacti 1.2.12 allows an admin to inject SQL via the filter parameter. This can lead to remote command execution because the product accepts stacked queries.	7.2	More Details
CVE-2020-12827	MJML prior to 4.6.3 contains a path traversal vulnerability when processing the mj-include directive within an MJML document.	7.2	More Details
CVE-2019-20842	An issue was discovered in Mattermost Server before 5.18.0, 5.17.2, 5.16.4, 5.15.4, and 5.9.7. There is SQL injection by admins via SearchAllChannels.	7.2	More Details
CVE-2020-3277	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	7.2	More Details
CVE-2020-14990	IOBit Advanced SystemCare Free 13.5.0.263 allows local users to gain privileges for file deletion by manipulating the Clean & Optimize feature with an NTFS junction and an Object Manager symbolic link.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14974	The driver in IOBit Unlocker 1.1.2 allows a low-privileged user to unlock a file and kill processes (even ones running as SYSTEM) that hold a handle, via IOCTL code 0x222124.	7.1	More Details
CVE-2020-10750	Sensitive information written to a log file vulnerability was found in jaegertracing/jaeger before version 1.18.1 when the Kafka data store is used. This flaw allows an attacker with access to the container's log file to discover the Kafka credentials.	7.1	More Details
CVE-2020-14433	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25.	6.8	More Details
CVE-2020-14434	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	6.8	More Details
CVE-2020-3236	A vulnerability in the CLI of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files. The attacker would need valid administrative credentials. This vulnerability is due to improper input validation of CLI command arguments. An attacker could exploit this vulnerability by using path traversal techniques when executing a vulnerable command. A successful exploit could allow the attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files on an affected device.	6.7	More Details
CVE-2020-10740	A vulnerability was found in Wildfly in versions before 20.0.0.Final, where a remote deserialization attack is possible in the Enterprise Application Beans(EJB) due to lack of validation/filtering capabilities in wildfly.	6.6	More Details
CVE-2017-18874	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2 when local storage for files is used. A System Admin can achieve directory traversal.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11905	The Treck TCP/IP stack before 6.0.1.66 has a DHCPv6 Out-of-bounds Read.	6.5	More Details
CVE-2020-14455	An issue was discovered in Mattermost Desktop App before 4.4.0. Prompting for HTTP Basic Authentication is mishandled, allowing phishing, aka MMSA-2020-0007.	6.5	More Details
CVE-2018-21250	An issue was discovered in Mattermost Server before 5.2.2, 5.1.2, and 4.10.4. It allows remote attackers to cause a denial of service (memory consumption) via crafted image dimensions.	6.5	More Details
CVE-2020-8167	A CSRF vulnerability exists in rails <= 6.0.3 rails-ujs module that could allow attackers to send CSRF tokens to wrong domains.	6.5	More Details
CVE-2020-14460	An issue was discovered in Mattermost Server before 5.19.0, 5.18.1, 5.17.3, 5.16.5, and 5.9.8. Creation of a trusted OAuth application does not always require admin privileges, aka MMSA-2020-0001.	6.5	More Details
CVE-2020-10782	An exposure of sensitive information flaw was found in Ansible version 3.7.0. Sensitive information, such tokens and other secrets could be readable and exposed from the rsyslog configuration file, which has set the wrong world-readable permissions. The highest threat from this vulnerability is to confidentiality. This is fixed in Ansible version 3.7.1.	6.5	More Details
CVE-2016-11078	An issue was discovered in Mattermost Server before 3.0.0. It potentially allows attackers to obtain sensitive information (credential fields within config.json) via the System Console UI.	6.5	More Details
CVE-2020-14958	In Gogs 0.11.91, MakeEmailPrimary in models/user_mail.go lacks a "not the owner of the email" check.	6.5	More Details
CVE-2020-14401	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/scale.c has a pixel_value integer overflow.	6.5	More Details
CVE-2020-13157	modules\users\admin\edit.php in NukeViet 4.4 allows CSRF to change a user's password via an admin/index.php?nv=users&op=edit&userid= URI. The old password is not needed.	6.5	More Details
CVE-2020-13156	modules\users\admin\add_user.php in NukeViet 4.4 allows CSRF to add a user account via the admin/index.php?nv=users&op=user_add URI.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13961	Strapi before 3.0.2 could allow a remote authenticated attacker to bypass security restrictions because templates are stored in a global variable without any sanitation. By sending a specially crafted request, an attacker could exploit this vulnerability to update the email template for both password reset and account confirmation emails.	6.5	More Details
CVE-2020-1835	HUAWEI Mate 30 with versions earlier than 10.1.0.126(C00E125R5P3) have an information disclosure vulnerability. A logic judgment error occurs when the system handling Bluetooth connections, an attacker could craft as an authenticated Bluetooth peer to launch the attack. Successful exploit could cause information disclosure.	6.5	More Details
CVE-2020-13426	The Multi-Scheduler plugin 1.0.0 for WordPress has a Cross-Site Request Forgery (CSRF) vulnerability in the forms it presents, allowing the possibility of deleting records (users) when an ID is known.	6.5	More Details
CVE-2020-14405	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/rfbproto.c does not limit TextChat size.	6.5	More Details
CVE-2020-11903	The Treck TCP/IP stack before 6.0.1.28 has a DHCP Out-of-bounds Read.	6.5	More Details
CVE-2020-3241	A vulnerability in the orchestration tasks of Cisco UCS Director could allow an authenticated, remote attacker to perform a path traversal attack on an affected device. The vulnerability is due to insufficient validation of user-supplied input on the web-based management interface. An attacker could exploit this vulnerability by creating a task with specific configuration parameters. A successful exploit could allow the attacker to overwrite arbitrary files in the file system of an affected device.	6.5	More Details
CVE-2019-20873	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. It allows attackers to obtain sensitive information during user activation/deactivation.	6.5	More Details
CVE-2020-14470	In Octopus Deploy 2018.8.0 through 2019.x before 2019.12.2, an authenticated user with could trigger a deployment that leaks the Helm Chart repository password.	6.5	More Details
CVE-2016-11072	An issue was discovered in Mattermost Server before 3.0.2. The purposes of a session ID and a Session Token were mishandled.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20844	An issue was discovered in Mattermost Server before 5.18.0, 5.17.2, 5.16.4, 5.15.4, and 5.9.7. An attacker can spoof a direct-message channel by changing the type of a channel.	6.5	More Details
CVE-2020-1727	A vulnerability was found in Keycloak before 9.0.2, where every Authorization URL that points to an IDP server lacks proper input validation as it allows a wide range of characters. This flaw allows a malicious to craft deep links that introduce further attack scenarios on affected clients.	6.4	More Details
CVE-2020-5345	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an authorization bypass vulnerability. An authenticated malicious user may potentially execute commands to alter or stop database statistics.	6.4	More Details
CVE-2020-11907	The Treck TCP/IP stack before 6.0.1.66 improperly handles a Length Parameter Inconsistency in TCP.	6.3	More Details
CVE-2020-4068	In APNSwift 1.0.0, calling APNSwiftSigner.sign(digest:) is likely to result in a heap buffer overflow. This has been fixed in 1.0.1.	6.3	More Details
CVE-2020-11906	The Treck TCP/IP stack before 6.0.1.66 has an Ethernet Link Layer Integer Underflow.	6.3	More Details
CVE-2020-13277	An authorization issue in the mirroring logic allowed read access to private repositories in GitLab CE/EE 10.6 and later through 13.0.5	6.3	More Details
CVE-2020-13427	Victor CMS 1.0 has Persistent XSS in admin/users.php?source=add_user via the user_name, user_firstname, or user_lastname parameter.	6.1	More Details
CVE-2020-13262	Client-Side code injection through Mermaid markup in GitLab CE/EE 12.9 and later through 13.0.1 allows a specially crafted Mermaid payload to PUT requests on behalf of other users via clicking on a link	6.1	More Details
CVE-2016-11073	An issue was discovered in Mattermost Server before 3.0.0. It allows XSS via a Legal or Support setting.	6.1	More Details
CVE-2017-18893	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. Display names allow XSS.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18892	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. E-mail templates can have a field in which HTML content is not neutralized.	6.1	More Details
CVE-2016-11071	An issue was discovered in Mattermost Server before 3.1.0. It allows XSS because the noreferrer and noopener protection mechanisms were not in place.	6.1	More Details
CVE-2020-14446	An issue was discovered in WSO2 Identity Server through 5.10.0 and WSO2 IS as Key Manager through 5.10.0. An open redirect exists.	6.1	More Details
CVE-2017-18897	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5, when used as an OAuth 2.0 service provider. It mishandles a deny action for a redirection.	6.1	More Details
CVE-2016-11082	An issue was discovered in Mattermost Server before 2.2.0. It allows XSS via a crafted link.	6.1	More Details
CVE-2017-18907	An issue was discovered in Mattermost Server before 4.0.0, 3.10.2, and 3.9.2. XSS could occur via a channel header.	6.1	More Details
CVE-2016-11083	An issue was discovered in Mattermost Server before 2.2.0. It allows XSS because it configures files to be opened in a browser window.	6.1	More Details
CVE-2016-11084	An issue was discovered in Mattermost Server before 2.1.0. It allows XSS via CSRF.	6.1	More Details
CVE-2017-18921	An issue was discovered in Mattermost Server before 3.6.0 and 3.5.2. XSS can occur via a link on an error page.	6.1	More Details
CVE-2017-18904	An issue was discovered in Mattermost Server before 4.0.0, 3.10.2, and 3.9.2. It allows XSS via an uploaded file.	6.1	More Details
CVE-2016-11063	An issue was discovered in Mattermost Server before 3.5.1. XSS can occur via file preview.	6.1	More Details
CVE-2017-18913	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. XSS can occur via a link on an error page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18891	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. It allows Phishing because an error page can have a link.	6.1	More Details
CVE-2020-14202	WebFOCUS Business Intelligence 8.0 (SP6) was prone to XSS via arbitrary URL parameters.	6.1	More Details
CVE-2016-11079	An issue was discovered in Mattermost Server before 3.0.0. It allows XSS via a redirect URL.	6.1	More Details
CVE-2020-14475	A reflected cross-site scripting (XSS) vulnerability in Dolibarr 11.0.3 allows remote attackers to inject arbitrary web script or HTML into public/notice.php (related to transphrase and transkey).	6.1	More Details
CVE-2017-18877	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. XSS attacks could occur against an OAuth 2.0 allow/deny page.	6.1	More Details
CVE-2020-14454	An issue was discovered in Mattermost Desktop App before 4.4.0. Attackers can open web pages in the desktop application because server redirection is mishandled, aka MMSA-2020-0008.	6.1	More Details
CVE-2017-18882	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. XSS can occur via OpenGraph data.	6.1	More Details
CVE-2017-18881	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. XSS could occur via a goto_location response to a slash command.	6.1	More Details
CVE-2017-18880	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. XSS could occur via the title_link field of a Slack attachment.	6.1	More Details
CVE-2017-18879	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. XSS could occur via the author_link field of a Slack attachment.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3337	A vulnerability in the web server of Cisco Umbrella could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. The vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request that could cause the web application to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to redirect a user to a malicious website.	6.1	More Details
CVE-2020-14973	The loginForm within the general/login.php webpage in webTareas 2.0p8 suffers from a Reflected Cross Site Scripting (XSS) vulnerability via the query string.	6.1	More Details
CVE-2020-14408	An issue was discovered in Agentejo Cockpit 0.10.2. Insufficient sanitization of the to parameter in the /auth/login route allows for injection of arbitrary JavaScript code into a web page's content, creating a Reflected XSS attack vector.	6.1	More Details
CVE-2020-3356	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by interacting with the interface in a way that injects malicious content in a log file. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2019-3865	A vulnerability was found in quay-2, where a stored XSS vulnerability has been found in the super user function of quay. Attackers are able to use the name field of service key to inject scripts and make it run when admin users try to change the name.	6.1	More Details
CVE-2020-9438	Tinxy Door Lock with firmware before 3.2 allow attackers to unlock a door by replaying an Unlock request that occurred when the attacker was previously authorized. In other words, door-access revocation is mishandled.	5.9	More Details
CVE-2020-14422	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. This is fixed in: v3.5.10, v3.5.10rc1; v3.6.12; v3.7.9; v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1; v3.9.0, v3.9.0b4, v3.9.0b5, v3.9.0rc1, v3.9.0rc2.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14981	The ThreatTrack VIPRE Password Vault app through 1.100.1090 for iOS has Missing SSL Certificate Validation.	5.9	More Details
CVE-2020-14954	Mutt before 1.14.4 and NeoMutt before 2020-06-19 have a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a man-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection."	5.9	More Details
CVE-2020-14980	The Sophos Secure Email application through 3.9.4 for Android has Missing SSL Certificate Validation.	5.9	More Details
CVE-2020-3368	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. The vulnerability is due to insufficient input validation of URLs. An attacker could exploit this vulnerability by crafting the URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for the affected device, which could allow malicious URLs to pass through the device.	5.8	More Details
CVE-2020-7932	OMERO.web before 5.6.3 optionally allows sensitive data elements (e.g., a session key) to be passed as URL query parameters. If an attacker tricks a user into clicking a malicious link in OMERO.web, the information in the query parameters may be exposed in the Referer header seen by the target. Information in the URL path such as object IDs may also be exposed.	5.7	More Details
CVE-2019-14092	System Services exports services without permission protect and can lead to information exposure in Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9207C, MDM9607, Rennell, Saipan, SM8150, SM8250, SXR2130	5.5	More Details
CVE-2019-20872	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. SSRF can attack local services.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-10626	Payload size is not validated before reading memory that may cause issue of accessing invalid pointer or some garbage data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Rennell, Saipan, SC8180X, SDA660, SDA845, SDM429W, SDM439, SDM670, SDM710, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	5.5	More Details
CVE-2019-20860	An issue was discovered in Mattermost Server before 5.14.0, 5.13.3, 5.12.6, and 5.9.4. It allows remote attackers to cause a denial of service (application hang) via a crafted SVG document.	5.5	More Details
CVE-2020-14976	GNS3 ubridge through 0.9.18 on macOS, as used in GNS3 server before 2.1.17, allows a local attacker to read arbitrary files because it handles configuration-file errors by printing the configuration file while executing in a setuid root context.	5.5	More Details
CVE-2020-3350	A vulnerability in the endpoint software of Cisco AMP for Endpoints and Clam AntiVirus could allow an authenticated, local attacker to cause the running software to delete arbitrary files on the system. The vulnerability is due to a race condition that could occur when scanning malicious files. An attacker with local shell access could exploit this vulnerability by executing a script that could trigger the race condition. A successful exploit could allow the attacker to delete arbitrary files on the system that the attacker would not normally have privileges to delete, producing system instability or causing the endpoint software to stop working.	5.5	More Details
CVE-2020-3347	A vulnerability in Cisco Webex Meetings Desktop App for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. The vulnerability is due to unsafe usage of shared memory that is used by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens that could aid the attacker in future attacks.	5.5	More Details
CVE-2020-13480	Verint Workforce Optimization (WFO) 15.2 allows HTML injection via the "send email" feature.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13888	Kordil EDMS through 2.2.60rc3 allows stored XSS in users_edit.php, users_management_edit.php, and user_management.php.	5.4	More Details
CVE-2020-14962	Multiple XSS vulnerabilities in the Final Tiles Gallery plugin before 3.4.19 for WordPress allow remote attackers to inject arbitrary web script or HTML via the Title (aka imageTitle) or Caption (aka description) field of an image to wp-admin/admin-ajax.php.	5.4	More Details
CVE-2020-14943	The Firstname and Lastname parameters in Global RADAR BSA Radar 1.6.7234.24750 and earlier are vulnerable to stored cross-site scripting (XSS) via Update User Profile.	5.4	More Details
CVE-2020-14073	XSS exists in PRTG Network Monitor 20.1.56.1574 via crafted map properties. An attacker with Read/Write privileges can create a map, and then use the Map Designer Properties screen to insert JavaScript code. This can be exploited against any user with View Maps or Edit Maps access.	5.4	More Details
CVE-2020-14959	Multiple XSS vulnerabilities in the Easy Testimonials plugin before 3.6 for WordPress allow remote attackers to inject arbitrary web script or HTML via the wp-admin/post.php Client Name, Position, Web Address, Other, Location Reviewed, Product Reviewed, Item Reviewed, or Rating parameter.	5.4	More Details
CVE-2020-9288	An improper neutralization of input vulnerability in FortiWLC 8.5.1 allows a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the ESS profile or the Radius Profile.	5.4	More Details
CVE-2020-11899	The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read.	5.4	More Details
CVE-2020-4297	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 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: 176474.	5.4	More Details
CVE-2020-14926	CMS Made Simple 2.2.14 allows XSS via a Search Term to the admin/moduleinterface.php?mact=ModuleManager page.	5.4	More Details
CVE-2020-14402	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/corre.c allows out-of-bounds access via encodings.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14403	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/hextile.c allows out-of-bounds access via encodings.	5.4	More Details
CVE-2020-14404	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rre.c allows out-of-bounds access via encodings.	5.4	More Details
CVE-2020-14444	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console Policy Administration user interface.	5.4	More Details
CVE-2020-14445	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console Basic Policy Editor user Interface.	5.4	More Details
CVE-2020-14462	CALDERA 2.7.0 allows XSS via the Operation Name box.	5.4	More Details
CVE-2020-4281	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 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: 176141.	5.4	More Details
CVE-2020-4295	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 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: 176408.	5.4	More Details
CVE-2019-20876	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. Users can deactivate themselves, bypassing a policy.	5.4	More Details
CVE-2016-11070	An issue was discovered in Mattermost Server before 3.1.0. It allows XSS via theme color-code values.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9495	Apache Archiva login service before 2.2.5 is vulnerable to LDAP injection. A attacker is able to retrieve user attribute data from the connected LDAP server by providing special values to the login form. With certain characters it is possible to modify the LDAP filter used to query the LDAP users. By measuring the response time for the login request, arbitrary attribute data can be retrieved from LDAP user objects.	5.3	More Details
CVE-2019-20869	An issue was discovered in Mattermost Server before 5.10.0, 5.9.1, 5.8.2, and 4.10.9. A non-member could change the Update/Patch Channel endpoint for a private channel.	5.3	More Details
CVE-2020-14457	An issue was discovered in Mattermost Server before 5.20.0. Non-members can receive broadcasted team details via the update_team WebSocket event, aka MMSA-2020-0012.	5.3	More Details
CVE-2019-20866	An issue was discovered in Mattermost Server before 5.12.0. Use of a Proxy HTTP header, rather than the source address in an IP packet header, for obtaining IP address information was mishandled.	5.3	More Details
CVE-2020-11912	The Treck TCP/IP stack before 6.0.1.66 has a TCP Out-of-bounds Read.	5.3	More Details
CVE-2019-20867	An issue was discovered in Mattermost Server before 5.11.0. An attacker can interfere with a channel's post loading via one crafted post.	5.3	More Details
CVE-2017-18914	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. An external link can occur on an error page even if it is not on an allowlist.	5.3	More Details
CVE-2017-18905	An issue was discovered in Mattermost Server before 4.0.0, 3.10.2, and 3.9.2, when used as an OAuth 2.0 service provider, Session invalidation was mishandled.	5.3	More Details
CVE-2019-20850	An issue was discovered in Mattermost Mobile Apps before 1.26.0. A view cache can persist on a device after a logout.	5.3	More Details
CVE-2016-11076	An issue was discovered in Mattermost Server before 3.0.0. It does not ensure that a cookie is used over SSL.	5.3	More Details
CVE-2018-21257	An issue was discovered in Mattermost Server before 5.1. It allows attackers to bypass intended access restrictions (for setting a channel header) via the Channel header slash command API.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7262	Improper Access Control vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.10.0 allows local users to view sensitive files via a carefully crafted HTTP request parameter.	5.3	More Details
CVE-2018-21259	An issue was discovered in Mattermost Server before 4.10.1, 4.9.4, and 4.8.2. It allows attackers to cause a denial of service (application hang) via a malformed link in a channel.	5.3	More Details
CVE-2020-11910	The Treck TCP/IP stack before 6.0.1.66 has an ICMPv4 Out-of-bounds Read.	5.3	More Details
CVE-2018-21265	An issue was discovered in Mattermost Desktop App before 4.0.0. It mishandled the Same Origin Policy for setPermissionRequestHandler (e.g., video, audio, and notifications).	5.3	More Details
CVE-2020-14452	An issue was discovered in Mattermost Server before 5.21.0. mmctl allows directory traversal via HTTP, aka MMSA-2020-0014.	5.3	More Details
CVE-2019-20849	An issue was discovered in Mattermost Mobile Apps before 1.26.0. Cookie data can persist on a device after a logout.	5.3	More Details
CVE-2019-20877	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. It allows attackers to obtain sensitive information about whether someone has 2FA enabled.	5.3	More Details
CVE-2019-20847	An issue was discovered in Mattermost Server before 5.18.0. An attacker can send a user_typing WebSocket event to any channel.	5.3	More Details
CVE-2016-11067	An issue was discovered in Mattermost Server before 3.2.0. It allowed crafted posts that could cause a web browser to hang.	5.3	More Details
CVE-2016-11068	An issue was discovered in Mattermost Server before 3.2.0. Attackers could read LDAP fields via injection.	5.3	More Details
CVE-2020-11913	The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14423	Convos before 4.20 does not properly generate a random secret in Core/Settings.pm and Util.pm. This leads to a predictable CONVOS_LOCAL_SECRET value, affecting password resets and invitations.	5.3	More Details
CVE-2020-3364	A vulnerability in the access control list (ACL) functionality of the standby route processor management interface of Cisco IOS XR Software could allow an unauthenticated, remote attacker to reach the configured IP addresses on the standby route processor management Gigabit Ethernet Management interface. The vulnerability is due to a logic error that was introduced in the Cisco IOS XR Software, which prevents the ACL from working when applied against the standby route processor management interface. An attacker could exploit this vulnerability by attempting to access the device through the standby route processor management interface.	5.3	More Details
CVE-2020-3360	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device.	5.3	More Details
CVE-2016-11075	An issue was discovered in Mattermost Server before 3.0.0. It allows attackers to obtain sensitive information about team URLs via an API.	5.3	More Details
CVE-2019-16245	OMERO before 5.6.1 makes the details of each user available to all users.	5.3	More Details
CVE-2020-3245	A vulnerability in the web application of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to create arbitrary user accounts. The vulnerability is due to the lack of authorization controls in the web application. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to add user accounts to the configuration of an affected device. These accounts would not be administrator or operator accounts.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3244	A vulnerability in the Enhanced Charging Service (ECS) functionality of Cisco ASR 5000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass the traffic classification rules on an affected device. The vulnerability is due to insufficient input validation of user traffic going through an affected device. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to bypass the traffic classification rules and potentially avoid being charged for traffic consumption.	5.3	More Details
CVE-2020-4188	IBM Security Guardium 10.6 and 11.1 may use insufficiently random numbers or values in a security context that depends on unpredictable numbers. IBM X-Force ID: 174807.	5.3	More Details
CVE-2020-4532	IBM Business Automation Workflow and IBM Business Process Manager (IBM Business Process Manager Express 8.5.5, 8.5.6, 8.5.7, and 8.6) could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 182716.	5.3	More Details
CVE-2019-20875	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. It allows a password reset to proceed while an e-mail address is being changed.	5.3	More Details
CVE-2020-11911	The Treck TCP/IP stack before 6.0.1.66 has Improper ICMPv4 Access Control.	5.3	More Details
CVE-2020-4028	Versions before 8.9.1, Various resources in Jira responded with a 404 instead of redirecting unauthenticated users to the login page, in some situations this may have allowed unauthorised attackers to determine if certain resources exist or not through an Information Disclosure vulnerability.	5.3	More Details
CVE-2017-18895	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. It allows attackers to obtain sensitive information (user statuses) via a REST API version 4 endpoint.	5.3	More Details
CVE-2017-18901	An issue was discovered in Mattermost Server before 4.1.0, 4.0.4, and 3.10.3. It allows attackers to discover a team invite ID by requesting a JSON document.	5.3	More Details
CVE-2017-18887	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It discloses the team creator's e-mail address to members.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18873	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It allows attackers to cause a denial of service (channel invisibility) via a misformatted post.	5.3	More Details
CVE-2020-11909	The Treck TCP/IP stack before 6.0.1.66 has an IPv4 Integer Underflow.	5.3	More Details
CVE-2017-18902	An issue was discovered in Mattermost Server before 4.1.0, 4.0.4, and 3.10.3. It allows attackers to discover team invite IDs via team API endpoints.	5.3	More Details
CVE-2017-18896	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. It allows attackers to add DEBUG lines to the logs via a REST API version 3 logging endpoint.	5.3	More Details
CVE-2017-18919	An issue was discovered in Mattermost Server before 3.7.0 and 3.6.3. Attackers can use the API for unauthenticated team creation.	5.3	More Details
CVE-2016-11062	An issue was discovered in Mattermost Server before 3.5.1. E-mail address verification can be bypassed.	5.3	More Details
CVE-2020-13261	Amazon EKS credentials disclosure in GitLab CE/EE 12.6 and later through 13.0.1 allows other administrators to view Amazon EKS credentials via HTML source code	5.3	More Details
CVE-2017-18899	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. It mishandles IP-based rate limiting.	5.3	More Details
CVE-2020-13264	Kubernetes cluster token disclosure in GitLab CE/EE 10.3 and later through 13.0.1 allows other group maintainers to view Kubernetes cluster token	5.3	More Details
CVE-2017-18898	An issue was discovered in Mattermost Server before 4.2.0, 4.1.1, and 4.0.5. It allows crafted posts that potentially cause a web browser to hang.	5.3	More Details
CVE-2020-14961	Concrete5 before 8.5.3 does not constrain the sort direction to a valid asc or desc value.	5.3	More Details
CVE-2017-18916	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. API endpoint access control does not honor an integration permission restriction.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20889	An issue was discovered in Mattermost Server before 5.7, 5.6.3, 5.5.2, and 4.10.5. It mishandles permissions for user-access token creation.	5.3	More Details
CVE-2019-20884	An issue was discovered in Mattermost Server before 5.8.0. It allows attackers to partially attach a file to more than one post.	5.3	More Details
CVE-2019-20882	An issue was discovered in Mattermost Server before 5.8.0. It does not honor the domain requirement when processing a join request for an open team.	5.3	More Details
CVE-2020-11068	In LoRaMac-node before 4.4.4, a reception buffer overflow can happen due to the received buffer size not being checked. This has been fixed in 4.4.4.	5.0	More Details
CVE-2017-18875	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2 when local storage for files is used. A System Admin can create arbitrary files.	4.9	More Details
CVE-2017-18918	An issue was discovered in Mattermost Server before 3.7.3 and 3.6.5. A System Administrator can place a SAML certificate at an arbitrary pathname.	4.9	More Details
CVE-2020-8618	An attacker who is permitted to send zone data to a server via zone transfer can exploit this to intentionally trigger the assertion failure with a specially constructed zone, denying service to clients.	4.9	More Details
CVE-2020-3242	A vulnerability in the REST API of Cisco UCS Director could allow an authenticated, remote attacker with administrative privileges to obtain confidential information from an affected device. The vulnerability exists because confidential information is returned as part of an API response. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to obtain the API key of another user, which would allow the attacker to impersonate the account of that user on the affected device. To exploit this vulnerability, the attacker must have administrative privileges on the device.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8619	In ISC BIND9 versions BIND 9.11.14 -> 9.11.19, BIND 9.14.9 -> 9.14.12, BIND 9.16.0 -> 9.16.3, BIND Supported Preview Edition 9.11.14-S1 -> 9.11.19-S1: Unless a nameserver is providing authoritative service for one or more zones and at least one zone contains an empty non-terminal entry containing an asterisk ("*") character, this defect cannot be encountered. A would-be attacker who is allowed to change zone content could theoretically introduce such a record in order to exploit this condition to cause denial of service, though we consider the use of this vector unlikely because any such attack would require a significant privilege level and be easily traceable.	4.9	More Details
CVE-2017-18876	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2 when local storage for files is used. A System Admin can test for the existence of an arbitrary file.	4.9	More Details
CVE-2020-3355	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need administrative credentials on the affected device.	4.8	More Details
CVE-2020-3354	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need administrative credentials on the affected device.	4.8	More Details
CVE-2020-14927	Navigate CMS 2.9 allows XSS via the Alias or Real URL field of the "Web Sites > Create > Aliases > Add" screen.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14965	On TP-Link TL-WR740N v4 and TL-WR740ND v4 devices, an attacker with access to the admin panel can inject HTML code and change the HTML context of the target pages and stations in the access-control settings via targets_lists_name or hosts_lists_name. The vulnerability can also be exploited through a CSRF, requiring no authentication as an administrator.	4.8	More Details
CVE-2020-3362	A vulnerability in the CLI of Cisco Network Services Orchestrator (NSO) could allow an authenticated, local attacker to access confidential information on an affected device. The vulnerability is due to a timing issue in the processing of CLI commands. An attacker could exploit this vulnerability by executing a specific sequence of commands on the CLI. A successful exploit could allow the attacker to read configuration information that would normally be accessible to administrators only.	4.7	More Details
CVE-2020-4070	In CSS Validator less than or equal to commit 54d68a1, there is a cross-site scripting vulnerability in handling URIs. A user would have to click on a specifically crafted validator link to trigger it. This has been patched in commit e5c09a9.	4.6	More Details
CVE-2020-1834	HUAWEI P30 and HUAWEI P30 Pro with versions earlier than 10.1.0.135(C00E135R2P11) and versions earlier than 10.1.0.135(C00E135R2P8) have an insufficient integrity check vulnerability. The system does not check certain software package's integrity sufficiently. Successful exploit could allow an attacker to load a crafted software package to the device.	4.6	More Details
CVE-2020-11914	The Treck TCP/IP stack before 6.0.1.66 has an ARP Out-of-bounds Read.	4.3	More Details
CVE-2016-11080	An issue was discovered in Mattermost Server before 3.0.0. It offers superfluous APIs for a Team Administrator to view account details.	4.3	More Details
CVE-2016-11081	An issue was discovered in Mattermost Server before 2.2.0. It allows unintended access to information stored by a web browser.	4.3	More Details
CVE-2020-14946	downloadFile.ashx in the Administrator section of the Surveillance module in Global RADAR BSA Radar 1.6.7234.24750 and earlier allows users to download transaction files. When downloading the files, a user is able to view local files on the web server by manipulating the FileName and FilePath parameters in the URL, or while using a proxy. This vulnerability could be used to view local sensitive files or configuration files.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18910	An issue was discovered in Mattermost Server before 3.8.2, 3.7.5, and 3.6.7. E-mail notifications can have spoofed links.	4.3	More Details
CVE-2019-20879	An issue was discovered in Mattermost Server before 5.8.0, 5.7.2, 5.6.5, and 4.10.7. Changes to e-mail addresses do not require credential re-entry.	4.3	More Details
CVE-2019-20870	An issue was discovered in Mattermost Server before 5.10.0. An attacker can bypass the intended appearance of the Edited flag after changing a post's file ID.	4.3	More Details
CVE-2016-11065	An issue was discovered in Mattermost Server before 3.3.0. An attacker could use the WebSocket feature to send pop-up messages to users or change a post's appearance.	4.3	More Details
CVE-2019-20883	An issue was discovered in Mattermost Server before 5.8.0, when Town Square is set to Read-Only. Users can pin or unpin a post.	4.3	More Details
CVE-2018-21261	An issue was discovered in Mattermost Server before 4.8.1, 4.7.4, and 4.6.3. An e-mail invite accidentally included the team invite_id, which leads to unintended excessive invitation privileges.	4.3	More Details
CVE-2019-20887	An issue was discovered in Mattermost Server before 5.7.1, 5.6.4, 5.5.3, and 4.10.6. It does not honor flags API permissions when deciding whether a user can receive intra-team posts.	4.3	More Details
CVE-2019-20890	An issue was discovered in Mattermost Server before 5.7. It allows a bypass of e-mail address discovery restrictions.	4.3	More Details
CVE-2018-21255	An issue was discovered in Mattermost Server before 5.1. Non-members of a channel could use the Channel PATCH API to modify that channel.	4.3	More Details
CVE-2018-21254	An issue was discovered in Mattermost Server before 5.1. An attacker can bypass intended access control (for direct-message channel creation) via the Message slash command.	4.3	More Details
CVE-2018-21253	An issue was discovered in Mattermost Server before 5.1, 5.0.2, and 4.10.2. An attacker could use the invite_people slash command to invite a non-permitted user.	4.3	More Details
CVE-2017-18870	An issue was discovered in Mattermost Server before 4.5.0, 4.4.5, and 4.3.4. It mishandled webhook access control in the EnableOnlyAdminIntegrations case.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-18878	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. Knowledge of a session ID allows revoking another user's session.	4.3	More Details
CVE-2020-13265	User email verification bypass in GitLab CE/EE 12.5 and later through 13.0.1 allows user to bypass email verification	4.3	More Details
CVE-2017-18872	An issue was discovered in Mattermost Server before 4.4.3 and 4.3.3. Attackers could reconfigure an OAuth app in some cases where Mattermost is an OAuth 2.0 service provider.	4.3	More Details
CVE-2018-21252	An issue was discovered in Mattermost Server before 5.2, 5.1.1, 5.0.3, and 4.10.3. Attackers could use multiple e-mail addresses to bypass a domain-based policy for signups.	4.3	More Details
CVE-2018-21256	An issue was discovered in Mattermost Server before 5.1. It allows attackers to bypass intended access restrictions (for group-message channel creation) via the Group message slash command.	4.3	More Details
CVE-2020-11908	The Treck TCP/IP stack before 4.7.1.27 mishandles '\0' termination in DHCP.	4.3	More Details
CVE-2019-20878	An issue was discovered in Mattermost Server before 5.9.0, 5.8.1, 5.7.3, and 4.10.8. Changes, within the application, to e-mail addresses are mishandled.	4.3	More Details
CVE-2017-18889	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. An attacker could create fictive system-message posts via webhooks and slash commands, in the v3 or v4 REST API.	4.3	More Details
CVE-2017-18890	An issue was discovered in Mattermost Server before 4.3.0, 4.2.1, and 4.1.2. It allows an attacker to create a button that, when pressed by a user, launches an API request.	4.3	More Details
CVE-2020-13882	CISOfy Lynis before 3.0.0 has Incorrect Access Control because of a TOCTOU race condition. The routine to check the log and report file permissions was not working as intended and could be bypassed locally. Because of the race, an unprivileged attacker can set up a log and report file, and control that up to the point where the specific routine is doing its check. After that, the file can be removed, recreated, and used for additional attacks.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14416	In the Linux kernel before 5.4.16, a race condition in tty->disc_data handling in the slip and slcan line discipline could lead to a use-after-free, aka CID-0ace17d56824. This affects drivers/net/slip/slip.c and drivers/net/can/slcan.c.	4.2	More Details
CVE-2020-4060	In LoRa Basics Station before 2.0.4, there is a Use After Free vulnerability that leads to memory corruption. This bug is triggered on 32-bit machines when the CUPS server responds with a message (https://doc.sm.tc/station/cupsproto.html#http-post-response) where the signature length is larger than 2 GByte (never happens in practice), or the response is crafted specifically to trigger this issue (i.e. the length signature field indicates a value larger than (2**31)-1 although the signature actually does not contain that much data). In such a scenario, on 32 bit machines, Basic Station would execute a code path, where a piece of memory is accessed after it has been freed, causing the process to crash and restarted again. The CUPS transaction is typically mutually authenticated over TLS. Therefore, in order to trigger this vulnerability, the attacker would have to gain access to the CUPS server first. If the user chose to operate without authentication over TLS but yet is concerned about this vulnerability, one possible workaround is to enable TLS authentication. This has been fixed in 2.0.4.	4.1	More Details
CVE-2020-6752	In OMERO before 5.6.1, group owners can access members' data in other groups.	3.8	More Details
CVE-2020-4066	In Limdu before 0.95, the trainBatch function has a command injection vulnerability. Clients of the Limdu library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. This has been patched in 0.95.	3.8	More Details
CVE-2018-21249	An issue was discovered in Mattermost Server before 5.3.0. It mishandles timing.	3.7	More Details
CVE-2020-4031	In FreeRDP before version 2.1.2, there is a use-after-free in gdi_SelectObject. All FreeRDP clients using compatibility mode with /relax-order-checks are affected. This is fixed in version 2.1.2.	3.5	More Details
CVE-2020-4030	In FreeRDP before version 2.1.2, there is an out of bounds read in TrioParse. Logging might bypass string length checks due to an integer overflow. This is fixed in version 2.1.2.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11099	In FreeRDP before version 2.1.2, there is an out of bounds read in license_read_new_or_upgrade_license_packet. A manipulated license packet can lead to out of bound reads to an internal buffer. This is fixed in version 2.1.2.	3.5	More Details
CVE-2020-11098	In FreeRDP before version 2.1.2, there is an out-of-bound read in glyph_cache_put. This affects all FreeRDP clients with `+glyph-cache` option enabled This is fixed in version 2.1.2.	3.5	More Details
CVE-2020-11097	In FreeRDP before version 2.1.2, an out of bounds read occurs resulting in accessing a memory location that is outside of the boundaries of the static array PRIMARY_DRAWING_ORDER_FIELD_BYTES. This is fixed in version 2.1.2.	3.5	More Details
CVE-2020-11096	In FreeRDP before version 2.1.2, there is a global OOB read in update_read_cache_bitmap_v3_order. As a workaround, one can disable bitmap cache with -bitmap-cache (default). This is fixed in version 2.1.2.	3.5	More Details
CVE-2020-11095	In FreeRDP before version 2.1.2, an out of bound reads occurs resulting in accessing a memory location that is outside of the boundaries of the static array PRIMARY_DRAWING_ORDER_FIELD_BYTES. This is fixed in version 2.1.2.	3.5	More Details
CVE-2020-3972	VMware Tools for macOS (11.x.x and prior before 11.1.1) contains a denial-of-service vulnerability in the Host-Guest File System (HGFS) implementation. Successful exploitation of this issue may allow attackers with non-admin privileges on guest macOS virtual machines to create a denial-of-service condition on their own VMs.	3.3	More Details
CVE-2019-13033	In CISOfy Lynis 2.x through 2.7.5, the license key can be obtained by looking at the process list when a data upload is being performed. This license can be used to upload data to a central Lynis server. Although no data can be extracted by knowing the license key, it may be possible to upload the data of additional scans.	3.3	More Details
CVE-2020-4033	In FreeRDP before version 2.1.2, there is an out of bounds read in RLEDECOMPRESS. All FreeRDP based clients with sessions with color depth < 32 are affected. This is fixed in version 2.1.2.	3.1	More Details
CVE-2020-4032	In FreeRDP before version 2.1.2, there is an integer casting vulnerability in update_recv_secondary_order. All clients with +glyph-cache /relax-order-checks are affected. This is fixed in version 2.1.2.	3.1	More Details
CVE-2016-11077	An issue was discovered in Mattermost Server before 3.0.0. It has a superfluous API in which the System Admin can change the account name and e-mail address of an LDAP account.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-21260	An issue was discovered in Mattermost Server before 4.8.1, 4.7.4, and 4.6.3. WebSocket events were accidentally sent during certain user-management operations, violating user privacy.	2.7	More Details
CVE-2020-14467	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-2020-10747	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