SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 03 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-2020-12493	An open port used for debugging in SWARCOs CPU LS4000 Series with versions starting with G4... grants root access to the device without access control via network. A malicious user could use this vulnerability to get access to the device and disturb operations with connected devices.	10.0	More Details
CVE-2020-11844	Incorrect Authorization vulnerability in Micro Focus Container Deployment Foundation component affects products: - Hybrid Cloud Management. Versions 2018.05 to 2019.11. - ArcSight Investigate. versions 2.4.0, 3.0.0 and 3.1.0. - ArcSight Transformation Hub. versions 3.0.0, 3.1.0, 3.2.0. - ArcSight Interset. version 6.0.0. - ArcSight ESM (when ArcSight Fusion 1.0 is installed). version 7.2.1. - Service Management Automation (SMA). versions 2018.05 to 2020.02 - Operation Bridge Suite (Containerized). Versions 2018.05 to 2020.02. - Network Operation Management. versions 2017.11 to 2019.11. - Data Center Automation Containerized. versions 2018.05 to 2019.11 - Identity Intelligence. versions 1.1.0 and 1.1.1. The vulnerability could be exploited to provide unauthorized access to the Container Deployment Foundation.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8967	There is an improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in php files of GESIO ERP. GESIO ERP all versions prior to 11.2 allows malicious users to retrieve all database information.	10.0	More Details
CVE-2020-8606	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow remote attackers to bypass authentication on affected installations of Trend Micro InterScan Web Security Virtual Appliance.	9.8	More Details
CVE-2019-6342	An access bypass vulnerability exists when the experimental Workspaces module in Drupal 8 core is enabled. This can be mitigated by disabling the Workspaces module. It does not affect any release other than Drupal 8.7.4.	9.8	More Details
CVE-2020-13693	An unauthenticated privilege-escalation issue exists in the bbPress plugin before 2.6.5 for WordPress when New User Registration is enabled.	9.8	More Details
CVE-2014-7173	FarLinX X25 Gateway through 2014-09-25 allows command injection via shell metacharacters to sysSaveMonitorData.php, fsx25MonProxy.php, syseditdate.php, iframeupload.php, or sysRestoreX25Cplt.php.	9.8	More Details
CVE-2014-7175	FarLinX X25 Gateway through 2014-09-25 allows attackers to write arbitrary data to fsUI.xyz via fsSaveUIPersistence.php.	9.8	More Details
CVE-2014-8941	Lexiglot through 2014-11-20 allows SQL injection via an admin.php?page=users&from_id= or admin.php?page=history&limit= URI.	9.8	More Details
CVE-2014-8945	admin.php?page=projects in Lexiglot through 2014-11-20 allows command injection via username and password fields.	9.8	More Details
CVE-2020-3615	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3633	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2020-3641	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2020-12017	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device’s vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system.	9.8	More Details
CVE-2020-11059	In AEgir greater than or equal to 21.7.0 and less than 21.10.1, aegir publish and aegir build may leak secrets from environment variables in the browser bundle published to npm. This has been fixed in 21.10.1.	9.6	More Details
CVE-2020-6774	Improper Access Control in the Kiosk Mode functionality of Bosch Recording Station allows a local unauthenticated attacker to escape from the Kiosk Mode and access the underlying operating system.	9.3	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-13448	QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8 allows an authenticated remote attacker to execute code on the server via command injection in the servicestart parameter.	8.8	More Details
CVE-2020-13760	In Joomla! before 3.9.19, missing token checks in com_postinstall lead to CSRF.	8.8	More Details
CVE-2020-13642	An issue was discovered in the SiteOrigin Page Builder plugin before 2.10.16 for WordPress. The action_builder_content function did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The panels_data $_POST variable allows for malicious JavaScript to be executed in the victim's browser.	8.8	More Details
CVE-2020-13643	An issue was discovered in the SiteOrigin Page Builder plugin before 2.10.16 for WordPress. The live editor feature did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The live_editor_panels_data $_POST variable allows for malicious JavaScript to be executed in the victim's browser.	8.8	More Details
CVE-2020-11950	VIVOTEK Network Cameras before XXXXX-VVTK-2.2002.xx.01x (and before XXXXX-VVTK-0XXXX_Beta2) allows an authenticated user to upload and execute a script (with resultant execution of OS commands). For example, this affects IT9388-HT devices.	8.8	More Details
CVE-2020-13694	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user can execute sudo mysql without a password, which means that the www-data user can execute arbitrary OS commands via the mysql -e option.	8.8	More Details
CVE-2020-8605	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow remote attackers to execute arbitrary code on affected installations. Authentication is required to exploit this vulnerability.	8.8	More Details
CVE-2014-8942	Lexiglot through 2014-11-20 allows CSRF.	8.8	More Details
CVE-2020-13641	An issue was discovered in the Real-Time Find and Replace plugin before 4.0.2 for WordPress. The far_options_page function did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The find and replace rules could be updated with malicious JavaScript, allowing for that be executed later in the victims browser.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13229	An issue was discovered in Sysax Multi Server 6.90. A session can be hijacked if one observes the sid value in any /scgi URI, because it is an authentication token.	8.8	More Details
CVE-2020-1832	E6878-370 products with versions of 10.0.3.1(H557SP27C233) and 10.0.3.1(H563SP1C00) have a stack buffer overflow vulnerability. The program copies an input buffer to an output buffer without verification. An attacker in the adjacent network could send a crafted message, successful exploit could lead to stack buffer overflow which may cause malicious code execution.	8.8	More Details
CVE-2020-4018	The setup resources in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to complete the setup process via a cross-site request forgery (CSRF) vulnerability.	8.8	More Details
CVE-2020-12675	The mappress-google-maps-for-wordpress plugin before 2.54.6 for WordPress does not correctly implement capability checks for AJAX functions related to creation/retrieval/deletion of PHP template files, leading to Remote Code Execution. NOTE: this issue exists because of an incomplete fix for CVE-2020-12077.	8.8	More Details
CVE-2014-8943	Lexiglot through 2014-11-20 allows SSRF via the admin.php?page=projects svn_url parameter.	8.8	More Details
CVE-2020-11079	node-dns-sync (npm module dns-sync) through 0.2.0 allows execution of arbitrary commands . This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This has been fixed in 0.2.1.	8.6	More Details
CVE-2020-7660	serialize-javascript prior to 3.1.0 allows remote attackers to inject arbitrary code via the function "deleteFunctions" within "index.js".	8.1	More Details
CVE-2020-11039	In FreeRDP less than or equal to 2.0.0, when using a manipulated server with USB redirection enabled (nearly) arbitrary memory can be read and written due to integer overflows in length checks. This has been patched in 2.1.0.	8.0	More Details
CVE-2019-17603	Ene.sys in Asus Aura Sync through 1.07.71 does not properly validate input to IOCTL 0x80102044, 0x80102050, and 0x80102054, which allows local users to cause a denial of service (system crash) or gain privileges via IOCTL requests using crafted kernel addresses that trigger memory corruption.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13173	Initialization of the pcoip_credential_provider in Teradici PCoIP Standard Agent for Windows and PCoIP Graphics Agent for Windows versions 19.11.1 and earlier creates an insecure named pipe, which allows an attacker to intercept sensitive information or possibly elevate privileges via pre-installing an application which acquires that named pipe.	7.8	More Details
CVE-2020-3610	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2019-14054	Improper permissions in XBL_SEC region enable user to update XBL_SEC code and data and divert the RAM dump path to normal cold boot path in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM8150, SXR1130, SXR2130	7.8	More Details
CVE-2019-14087	Failure in buffer management while accessing handle for HDR blit when color modes not supported by display in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, QCS605	7.8	More Details
CVE-2019-14078	Out of bound memory access while processing qpay due to not validating length of the response buffer provided by User. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, MSM8909, MSM8998, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845	7.8	More Details
CVE-2020-7812	Ezhttptrans.ocx ActiveX Control in Kaoni ezHTTPTrans 1.0.0.70 and prior versions contain a vulnerability that could allow remote attacker to download arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution by rebooting the victim's PC.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14066	Integer overflow in calculating estimated output buffer size when getting a list of installed Feature IDs, Serial Numbers or checking Feature ID status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9205, MDM9607, Nicobar, QCS404, QCS405, Rennell, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SXR2130	7.8	More Details
CVE-2019-14077	Out of bound memory access while processing ese transmit command due to passing Response buffer received from user 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, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9607, MDM9650, MSM8909, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-3616	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150	7.8	More Details
CVE-2020-13634	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xF1002558	7.8	More Details
CVE-2020-10936	Sympa before 6.2.56 allows privilege escalation.	7.8	More Details
CVE-2020-3618	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3623	kernel failure due to load failures while running v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130	7.8	More Details
CVE-2020-3625	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130	7.8	More Details
CVE-2020-3630	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2014-8938	Lexiglot through 2014-11-20 allows local users to obtain sensitive information by listing a process because the username and password are on the command line.	7.8	More Details
CVE-2020-8482	Insecure storage of sensitive information in ABB Device Library Wizard versions 6.0.X, 6.0.3.1 and 6.0.3.2 allows unauthenticated low privilege user to read file that contains confidential data	7.8	More Details
CVE-2020-4019	The file editing functionality in the Atlassian Companion App before version 1.0.0 allows local attackers to have the app run a different executable in place of the app's cmd.exe via a untrusted search path vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11075	In Anchore Engine version 0.7.0, a specially crafted container image manifest, fetched from a registry, can be used to trigger a shell escape flaw in the anchore engine analyzer service during an image analysis process. The image analysis operation can only be executed by an authenticated user via a valid API request to anchore engine, or if an already added image that anchore is monitoring has its manifest altered to exploit the same flaw. A successful attack can be used to execute commands that run in the analyzer environment, with the same permissions as the user that anchore engine is run as - including access to the credentials that Engine uses to access its own database which have read-write ability, as well as access to the running engien analyzer service environment. By default Anchore Engine is released and deployed as a container where the user is non-root, but if users run Engine directly or explicitly set the user to 'root' then that level of access may be gained in the execution environment where Engine runs. This issue is fixed in version 0.7.1.	7.7	More Details
CVE-2014-9702	system/classes/DbPDO.php in Cmfive through 2015-03-15, when database connectivity malfunctions, allows remote attackers to obtain sensitive information (username and password) via any request, such as a password reset request.	7.5	More Details
CVE-2020-7654	All versions of snyk-broker before 4.73.1 are vulnerable to Information Exposure. It logs private keys if logging level is set to DEBUG.	7.5	More Details
CVE-2020-10739	Istio 1.4.x before 1.4.9 and Istio 1.5.x before 1.5.4 contain the following vulnerability when telemetry v2 is enabled: by sending a specially crafted packet, an attacker could trigger a Null Pointer Exception resulting in a Denial of Service. This could be sent to the ingress gateway or a sidecar, triggering a null pointer exception which results in a denial of service. This also affects servicemesh-proxy where a null pointer exception flaw was found in servicemesh-proxy. When running Telemetry v2 (not on by default in version 1.4.x), an attacker could send a specially crafted packet to the ingress gateway or proxy sidecar, triggering a denial of service.	7.5	More Details
CVE-2020-13757	Python-RSA before 4.1 ignores leading '\0' bytes during decryption of ciphertext. This could conceivably have a security-relevant impact, e.g., by helping an attacker to infer that an application uses Python-RSA, or if the length of accepted ciphertext affects application behavior (such as by causing excessive memory allocation).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12062	The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not fail under normal circumstances.	7.5	More Details
CVE-2020-1870	There is a denial of service vulnerability in some Huawei products. Due to improper memory management, memory leakage may occur in some special cases. Attackers can perform a series of operations to exploit this vulnerability. Successful exploit may cause a denial of service. Affected product versions include: CloudEngine 12800 versions V200R019C00SPC800; CloudEngine 5800 versions V200R019C00SPC800; CloudEngine 6800 versions V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R019C00SPC800; NE40E versions V800R011C00SPC200, V800R011C00SPC300, V800R011C10SPC100; NE40E-F versions V800R011C00SPC200, V800R011C10SPC100; NE40E-M versions V800R011C00SPC200, V800R011C10SPC100.	7.5	More Details
CVE-2020-7659	reel through 0.6.1 allows Request Smuggling attacks due to incorrect Content-Length and Transfer encoding header parsing. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks. Note: This project is deprecated, and is not maintained any more.	7.5	More Details
CVE-2020-13623	JerryScript 2.2.0 allows attackers to cause a denial of service (stack consumption) via a proxy operation.	7.5	More Details
CVE-2020-4367	IBM Planning Analytics Local 2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179001.	7.5	More Details
CVE-2014-8937	Lexiglot through 2014-11-20 allows denial of service because api/update.php launches svn update operations that use a great deal of resources.	7.5	More Details
CVE-2020-13622	JerryScript 2.2.0 allows attackers to cause a denial of service (assertion failure) because a property key query for a Proxy object returns unintended data.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6937	A Denial of Service vulnerability in MuleSoft Mule CE/EE 3.8.x, 3.9.x, and 4.x released before April 7, 2020, could allow remote attackers to submit data which can lead to resource exhaustion.	7.5	More Details
CVE-2020-13649	parser/js/js-scanner.c in JerryScript 2.2.0 mishandles errors during certain out-of-memory conditions, as demonstrated by a scanner_reverse_info_list NULL pointer dereference and a scanner_scan_all assertion failure.	7.5	More Details
CVE-2020-4232	IBM Security Identity Governance and Intelligence 5.2.6 could allow an attacker to enumerate usernames to find valid login credentials which could be used to attempt further attacks against the system. IBM X-Force ID: 175336.	7.5	More Details
CVE-2020-7663	websocket-extensions ruby module prior to 0.1.5 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.	7.5	More Details
CVE-2020-7662	websocket-extensions npm module prior to 0.1.4 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.	7.5	More Details
CVE-2020-4349	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 178423.	7.5	More Details
CVE-2020-4379	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179158.	7.5	More Details
CVE-2020-13759	rust-vmm vm-memory before 0.1.1 and 0.2.x before 0.2.1 allows attackers to cause a denial of service (loss of IP networking) because read_obj and write_obj do not properly access memory. This affects aarch64 (with musl or glibc) and x86_64 (with musl).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5410	Spring Cloud Config, versions 2.2.x prior to 2.2.3, versions 2.1.x prior to 2.1.9, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.	7.5	More Details
CVE-2020-13763	In Joomla! before 3.9.19, the default settings of the global textfilter configuration do not block HTML inputs for Guest users.	7.5	More Details
CVE-2020-4226	IBM MobileFirst Platform Foundation 8.0.0.0 stores highly sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 175207.	7.5	More Details
CVE-2020-3645	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130	7.5	More Details
CVE-2020-8604	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow remote attackers to disclose sensitive informatoin on affected installations.	7.5	More Details
CVE-2020-4350	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 178424.	7.5	More Details
CVE-2020-4245	IBM Security Identity Governance and Intelligence 5.2.6 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 175423.	7.5	More Details
CVE-2020-12607	An issue was discovered in fastecdsa before 2.1.2. When using the NIST P-256 curve in the ECDSA implementation, the point at infinity is mishandled. This means that for an extreme value in k and s^-1, the signature verification fails even if the signature is correct. This behavior is not solely a usability problem. There are some threat models where an attacker can benefit by successfully guessing users for whom signature verification will fail.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13764	common.php in the Gravity Forms plugin before 2.4.9 for WordPress can leak hashed passwords because user_pass is not considered a special case for a $current_user->get($property) call.	7.5	More Details
CVE-2020-13386	In SmartDraw 2020 27.0.0.0, the installer gives inherited write permissions to the Authenticated Users group on the SmartDraw 2020 installation folder. Additionally, when the product is installed, two scheduled tasks are created on the machine, SDMsgUpdate (Local) and SDMsgUpdate (TE). The scheduled tasks run in the context of the user who installed the product. Both scheduled tasks attempt to run the same binary, C:\SmartDraw 2020\Messages\SDNotify.exe. The folder Messages doesn't exist by default and (by extension) neither does SDNotify.exe. Due to the weak folder permissions, these can be created by any user. A malicious actor can therefore create a malicious SDNotify.exe binary, and have it automatically run, whenever the user who installed the product logs on to the machine. The malicious SDNotify.exe could, for example, create a new local administrator account on the machine.	7.3	More Details
CVE-2020-4020	The file downloading functionality in the Atlassian Companion App before version 1.0.0 allows remote attackers, who control a Confluence Server instance that the Companion App is connected to, execute arbitrary .exe files via a Protection Mechanism Failure.	7.2	More Details
CVE-2020-13695	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user has sudo privileges to execute grep as root without a password, which allows an attacker to obtain sensitive information via a grep of a /root/*.db or /etc/shadow file.	7.2	More Details
CVE-2020-8816	Pi-hole Web v4.3.2 (aka AdminLTE) allows Remote Code Execution by privileged dashboard users via a crafted DHCP static lease.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14053	When attempting to create a new XFRM policy, a stack out-of-bounds read will occur if the user provides a template where the mode is set to a value that does not resolve to a valid XFRM mode in Snapdragon Auto, Snapdragon Compute, 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, IPQ4019, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCA4531, QCN7605, QCS605, QM215, SA415M, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.1	More Details
CVE-2019-14043	Out of bound read in Fingerprint application due to requested data is being used without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9150, MDM9205, MDM9650, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.1	More Details
CVE-2019-14038	Buffer over-read in ADSP parse function due to lack of check for availability of sufficient data payload received in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710, SDM845, SDX20, SDX24	7.1	More Details
CVE-2020-5357	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-14042	Out of bound read in in fingerprint application due to requested data assigned to a local buffer without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9205, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.1	More Details
CVE-2019-14039	Out of bound read in adm call back function due to incorrect boundary check for payload in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710, SDM845, SDX20, SDX24	7.1	More Details
CVE-2020-4246	IBM Security Identity Governance and Intelligence 5.2.6 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 175481.	7.1	More Details
CVE-2020-3957	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior) and VMware Horizon Client for Mac (5.x and prior) contain a local privilege escalation vulnerability due to a Time-of-check Time-of-use (TOCTOU) issue in the service opener. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC and Horizon Client are installed.	7.0	More Details
CVE-2020-13630	ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.	7.0	More Details
CVE-2020-3680	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4352	IBM MQ on HPE NonStop 8.0.4 and 8.1.0 is vulnerable to a privilege escalation attack when running in restricted mode. IBM X-Force ID: 178427.	7.0	More Details
CVE-2020-11038	In FreeRDP less than or equal to 2.0.0, an Integer Overflow to Buffer Overflow exists. When using /video redirection, a manipulated server can instruct the client to allocate a buffer with a smaller size than requested due to an integer overflow in size calculation. With later messages, the server can manipulate the client to write data out of bound to the previously allocated buffer. This has been patched in 2.1.0.	6.9	More Details
CVE-2020-13754	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x mmio operation.	6.7	More Details
CVE-2020-6868	There is an input validation vulnerability in a PON terminal product of ZTE, which supports the creation of WAN connections through WEB management pages. The front-end limits the length of the WAN connection name that is created, but the HTTP proxy is available to be used to bypass the limitation. An attacker can exploit the vulnerability to tamper with the parameter value. This affects: ZTE F680 V9.0.10P1N6	6.5	More Details
CVE-2020-9071	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario.Affected product versions include:AR120-S versions V200R007C00SPC900,V200R007C00SPCa00	6.5	More Details
CVE-2019-15709	An improper input validation in FortiAP-S/W2 6.2.0 to 6.2.2, 6.0.5 and below, FortiAP-U 6.0.1 and below CLI admin console may allow unauthorized administrators to overwrite system files via specially crafted tcpdump commands in the CLI.	6.5	More Details
CVE-2020-7653	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network by creating symlinks to match whitelisted paths.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10703	A NULL pointer dereference was found in the libvirt API responsible introduced in upstream version 3.10.0, and fixed in libvirt 6.0.0, for fetching a storage pool based on its target path. In more detail, this flaw affects storage pools created without a target path such as network-based pools like gluster and RBD. Unprivileged users with a read-only connection could abuse this flaw to crash the libvirt daemon, resulting in a potential denial of service.	6.5	More Details
CVE-2020-7650	All versions of snyk-broker after 4.72.0 including and before 4.73.1 are vulnerable to Arbitrary File Read. It allows arbitrary file reads to users with access to Snyk's internal network of any files ending in the following extensions: yaml, yml or json.	6.5	More Details
CVE-2020-7648	All versions of snyk-broker before 4.72.2 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users who have access to Snyk's internal network by appending the URL with a fragment identifier and a whitelisted path e.g. `#package.json`	6.5	More Details
CVE-2020-13775	ZNC 1.8.0 up to 1.8.1-rc1 allows authenticated users to trigger an application crash (with a NULL pointer dereference) if echo-message is not enabled and there is no network.	6.5	More Details
CVE-2020-7652	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network via directory traversal.	6.5	More Details
CVE-2020-4249	IBM Security Identity Governance and Intelligence 5.2.6 could disclose highly sensitive information to other authenticated users on the sytem due to incorrect authorization. IBM X-Force ID: 175485.	6.5	More Details
CVE-2020-4348	IBM Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.4 could allow an authenticated GUI user to perform unauthorized actions due to missing function level access control. IBM X-Force ID: 178414	6.5	More Details
CVE-2020-4231	IBM Security Identity Governance and Intelligence 5.2.6 could allow an authenticated user to perform unauthorized commands due to hazardous input validation. IBM X-Force ID: 175335.	6.5	More Details
CVE-2020-11949	testserver.cgi of the web service on VIVOTEK Network Cameras before XXXXX-VVTK-2.2002.xx.01x (and before XXXXX-VVTK-0XXXX_Beta2) allows an authenticated user to obtain arbitrary files from a camera's local filesystem. For example, this affects IT9388-HT devices.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13645	In GNOME glib-networking through 2.64.2, the implementation of GTlsClientConnection skips hostname verification of the server's TLS certificate if the application fails to specify the expected server identity. This is in contrast to its intended documented behavior, to fail the certificate verification. Applications that fail to provide the server identity, including Balsa before 2.5.11 and 2.6.x before 2.6.1, accept a TLS certificate if the certificate is valid for any host.	6.5	More Details
CVE-2020-11017	In FreeRDP less than or equal to 2.0.0, by providing manipulated input a malicious client can create a double free condition and crash the server. This is fixed in version 2.1.0.	6.5	More Details
CVE-2020-11018	In FreeRDP less than or equal to 2.0.0, a possible resource exhaustion vulnerability can be performed. Malicious clients could trigger out of bound reads causing memory allocation with random size. This has been fixed in 2.1.0.	6.5	More Details
CVE-2020-11082	In Kaminari before 1.2.1, there is a vulnerability that would allow an attacker to inject arbitrary code into pages with pagination links. This has been fixed in 1.2.1.	6.4	More Details
CVE-2020-9291	An Insecure Temporary File vulnerability in FortiClient for Windows 6.2.1 and below may allow a local user to gain elevated privileges via exhausting the pool of temporary file names combined with a symbolic link attack.	6.3	More Details
CVE-2020-10737	A race condition was found in the mkhomedir tool shipped with the oddjob package in versions before 0.34.5 and 0.34.6 wherein, during the home creation, mkhomedir copies the /etc/skel directory into the newly created home and changes its ownership to the home's user without properly checking the homedir path. This flaw allows an attacker to leverage this issue by creating a symlink point to a target folder, which then has its ownership transferred to the new home directory's unprivileged user.	6.3	More Details
CVE-2019-11843	The MailPoet plugin before 3.23.2 for WordPress allows remote attackers to inject arbitrary web script or HTML using extra parameters in the URL (Reflective Server-Side XSS).	6.1	More Details
CVE-2018-18625	Grafana 5.3.1 has XSS via a link on the "Dashboard > All Panels > General" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	6.1	More Details
CVE-2018-18624	Grafana 5.3.1 has XSS via a column style on the "Dashboard > Table Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13628	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to host-monitoring/src/toolbar.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget.	6.1	More Details
CVE-2018-18623	Grafana 5.3.1 has XSS via the "Dashboard > Text Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	6.1	More Details
CVE-2020-10946	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the page parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget.	6.1	More Details
CVE-2020-13627	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget.	6.1	More Details
CVE-2020-10959	resources/src/mediawiki.page.ready/ready.js in MediaWiki before 1.35 allows remote attackers to force a logout and external redirection via HTML content in a MediaWiki page.	6.1	More Details
CVE-2020-13633	Fork before 5.8.3 allows XSS via navigation_title or title.	6.1	More Details
CVE-2020-8603	A cross-site scripting vulnerability (XSS) in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow a remote attacker to tamper with the web interface of affected installations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4366	IBM Planning Analytics Local 2.0 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: 178965.	6.1	More Details
CVE-2020-4503	IBM Planning Analytics Local 2.0 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: 182283.	6.1	More Details
CVE-2020-13228	An issue was discovered in Sysax Multi Server 6.90. There is reflected XSS via the /scgi sid parameter.	6.1	More Details
CVE-2020-13761	In Joomla! before 3.9.19, lack of input validation in the heading tag option of the "Articles - Newsflash" and "Articles - Categories" modules allows XSS.	6.1	More Details
CVE-2020-13762	In Joomla! before 3.9.19, incorrect input validation of the module tag option in com_modules allows XSS.	6.1	More Details
CVE-2020-13758	modules/security/classes/general.post_filter.php/post_filter.php in the Web Application Firewall in Bitrix24 through 20.0.950 allows XSS by placing %00 before the payload.	6.1	More Details
CVE-2020-4490	IBM Business Automation Workflow 18 and 19, and IBM Business Process Manager 8.0, 8.5, and 8.6 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a vitcim to a phishing site. IBM X-Force ID: 181989	6.1	More Details
CVE-2020-13401	An issue was discovered in Docker Engine before 19.03.11. An attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service.	6.0	More Details
CVE-2020-13245	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P.	5.9	More Details
CVE-2020-13253	sd_wp_addr in hw/sd/sd.c in QEMU 4.2.0 uses an unvalidated address, which leads to an out-of-bounds read during sdhci_write() operations. A guest OS user can crash the QEMU process.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13631	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter.c and build.c.	5.5	More Details
CVE-2020-12867	A NULL pointer dereference in sanei_epson_net_read in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075.	5.5	More Details
CVE-2019-20805	p_lx_elf.cpp in UPX before 3.96 has an integer overflow during unpacking via crafted values in a PT_DYNAMIC segment.	5.5	More Details
CVE-2020-13632	ext/fts3/fts3_snippet.c in SQLite before 3.32.0 has a NULL pointer dereference via a crafted matchinfo() query.	5.5	More Details
CVE-2020-3958	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.5.2) and VMware Fusion (11.x before 11.5.2) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with non-administrative access to a virtual machine to crash the virtual machine's vmx process leading to a denial of service condition.	5.5	More Details
CVE-2019-14067	Using non-time-constant functions like memcmp to compare sensitive data can lead to information leakage through timing side channel issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon 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, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	5.5	More Details
CVE-2020-4306	IBM Planning Analytics Local 2.0.0 through 2.0.9 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: 176735.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-8944	Lexiglot through 2014-11-20 allows XSS (Reflected) via the username, or XSS (Stored) via the admin.php?page=config install_name, intro_message, or new_file_content parameter.	5.4	More Details
CVE-2020-4419	IBM Jazz Reporting Service 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: 180071.	5.4	More Details
CVE-2020-4360	IBM Planning Analytics Local 2.0 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: 178765.	5.4	More Details
CVE-2020-4013	The review resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the review objectives.	5.4	More Details
CVE-2020-4431	IBM Planning Analytics Local 2.0 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: 180761.	5.4	More Details
CVE-2020-13644	An issue was discovered in the Accordion plugin before 2.2.9 for WordPress. The unprotected AJAX wp_ajax_accordions_ajax_import_json action allowed any authenticated user with Subscriber or higher permissions the ability to import a new accordion and inject malicious JavaScript as part of the accordion.	5.4	More Details
CVE-2020-4021	Affected versions are: Before 8.5.5, and from 8.6.0 before 8.8.1 of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the XML export view.	5.4	More Details
CVE-2020-4023	The review coverage resource in Atlassian Fisheye and Crucible before version 4.8.2 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the committerFilter parameter.	5.4	More Details
CVE-2020-4358	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178762.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-8940	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (names and details of projects) by visiting the /update.log URI.	5.3	More Details
CVE-2020-8330	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, preventing subsequent print jobs until the printer is rebooted.	5.3	More Details
CVE-2020-13227	An issue was discovered in Sysax Multi Server 6.90. An attacker can determine the username (under which the web server is running) by triggering an invalid path permission error. This bypasses the fakepath protection mechanism.	5.3	More Details
CVE-2014-7174	FarLinX X25 Gateway through 2014-09-25 allows directory traversal via the log-handling feature.	5.3	More Details
CVE-2020-8329	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, causing an error to be displayed and preventing printer from functioning until the printer is rebooted.	5.3	More Details
CVE-2020-10136	IP-in-IP protocol specifies IP Encapsulation within IP standard (RFC 2003, STD 1) that decapsulate and route IP-in-IP traffic is vulnerable to spoofing, access-control bypass and other unexpected behavior due to the lack of validation to verify network packets before decapsulation and routing.	5.3	More Details
CVE-2014-8939	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (full path) via an include/smarty/plugins/modifier.date_format.php request if PHP has a non-recommended configuration that produces warning messages.	5.3	More Details
CVE-2019-20807	In Vim before 8.1.0881, users can circumvent the rvim restricted mode and execute arbitrary OS commands via scripting interfaces (e.g., Python, Ruby, or Lua).	5.3	More Details
CVE-2020-4017	The /rest/jira-ril/1.0/jira-rest/applinks resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get information about any configured Jira application links via an information disclosure vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4233	IBM Security Identity Governance and Intelligence 5.2.6 could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for the session cookie in SSL mode. By intercepting its transmission within an HTTP session, an attacker could exploit this vulnerability to capture the cookie and obtain sensitive information. IBM X-Force ID: 175360.	5.3	More Details
CVE-2020-4016	The /plugins/servlet/jira-blockers/ resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get the ID of configured Jira application links via an information disclosure vulnerability.	5.3	More Details
CVE-2020-4244	IBM Security Identity Governance and Intelligence 5.2.6 could allow an unauthorized user to obtain sensitive information through user enumeration. IBM X-Force ID: 175422.	5.3	More Details
CVE-2020-4378	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 could allow a privileged authenticated user to perform unauthorized actions using a specially crated HTTP POST command. IBM X-Force ID: 179157.	4.9	More Details
CVE-2020-13660	CMS Made Simple through 2.2.14 allows XSS via a crafted File Picker profile name.	4.8	More Details
CVE-2020-1809	HUAWEI Mate 10 smartphones with versions earlier than 10.0.0.143(C00E143R2P4) have an information disclosure vulnerability. The attacker could wake up voice assistant then do a series of crafted voice operation, successful exploit could allow the attacker read certain files without unlock the phone leading to information disclosure.	4.6	More Details
CVE-2020-1798	HUAWEI P30 smartphones with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. A logic error occurs when handling NFC work, an attacker should establish a NFC connection to the target phone, and then do a series of operations on the target phone. Successful exploit could allow a guest user do certain operation which is beyond the guest user's privilege.	4.6	More Details
CVE-2020-5573	Android App 'kintone mobile for Android' 1.0.0 to 2.5 allows an attacker to obtain credential information registered in the product via unspecified vectors.	4.6	More Details
CVE-2020-5572	Android App 'Mailwise for Android' 1.0.0 to 1.0.1 allows an attacker to obtain credential information registered in the product via unspecified vectors.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20806	An issue was discovered in the Linux kernel before 5.2. There is a NULL pointer dereference in tw5864_handle_frame() in drivers/media/pci/tw5864/tw5864-video.c, which may cause denial of service, aka CID-2e7682ebfc75.	4.4	More Details
CVE-2020-4357	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 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: 178761.	4.3	More Details
CVE-2020-11019	In FreeRDP less than or equal to 2.0.0, when running with logger set to "WLOG_TRACE", a possible crash of application could occur due to a read of an invalid array index. Data could be printed as string to local terminal. This has been fixed in 2.1.0.	4.3	More Details
CVE-2020-7651	All versions of snyk-broker before 4.79.0 are vulnerable to Arbitrary File Read. It allows partial file reads for users who have access to Snyk's internal network via patch history from GitHub Commits API.	4.3	More Details
CVE-2020-10945	Centreon before 19.10.7 exposes Session IDs in server responses.	4.3	More Details
CVE-2020-4014	The /profile/deleteWatch.do resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to remove another user's watching settings for a repository via an improper authorization vulnerability.	4.3	More Details
CVE-2020-4015	The /json/fe/activeUserFinder.do resource in Altassian Fisheye and Crucible before version 4.8.1 allows remote attackers to view user user email addresses via a information disclosure vulnerability.	4.3	More Details
CVE-2020-13361	In QEMU 5.0.0 and earlier, es1370_transfer_audio in hw/audio/es1370.c does not properly validate the frame count, which allows guest OS users to trigger an out-of-bounds access during an es1370_write() operation.	3.9	More Details
CVE-2020-11089	In FreeRDP before 2.1.0, there is an out-of-bound read in irp functions (parallel_process_irp_create, serial_process_irp_create, drive_process_irp_write, printer_process_irp_write, rdpei_recv_pdu, serial_process_irp_write). This has been fixed in 2.1.0.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3959	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.1.0) and VMware Fusion (11.x before 11.1.0) contain a memory leak vulnerability in the VMCI module. A malicious actor with local non-administrative access to a virtual machine may be able to crash the virtual machine's vmx process leading to a partial denial of service.	3.3	More Details
CVE-2020-13362	In QEMU 5.0.0 and earlier, megasas_lookup_frame in hw/scsi/megasas.c has an out-of-bounds read via a crafted reply_queue_head field from a guest OS user.	3.2	More Details
CVE-2020-11087	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_AuthenticateMessage. This has been fixed in 2.1.0.	3.1	More Details
CVE-2020-11088	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_NegotiateMessage. This has been fixed in 2.1.0.	3.1	More Details
CVE-2020-11086	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_ntlm_v2_client_challenge that reads up to 28 bytes out-of-bound to an internal structure. This has been fixed in 2.1.0.	3.1	More Details
CVE-2020-4248	IBM Security Identity Governance and Intelligence 5.2.6 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: 175484.	2.7	More Details
CVE-2020-11085	In FreeRDP before 2.1.0, there is an out-of-bounds read in cliprdr_read_format_list. Clipboard format data read (by client or server) might read data out-of-bounds. This has been fixed in 2.1.0.	2.6	More Details
CVE-2020-13659	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer.	2.5	More Details
CVE-2020-1833	Honor 9X smartphones with versions earlier than 9.1.1.172(C00E170R8P1) have an improper authentication vulnerability. A logic error occurs when handling clock function, an attacker should do a series of crafted operations quickly before the phone is unlocked, successful exploit could allow the attacker to access clock information without unlock the phone.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1831	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.195(SP31C00E74R3P8) have an improper authorization vulnerability. The digital balance function does not sufficiently restrict the using time of certain user, successful exploit could allow the user break the limit of digital balance function after a series of operations with a PC.	2.4	More Details
CVE-2020-1797	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.185(C00E74R3P8) have an improper authorization vulnerability. The system does not properly restrict certain operation in ADB mode, successful exploit could allow certain user break the limit of digital balance function.	2.4	More Details
CVE-2020-11041	In FreeRDP less than or equal to 2.0.0, an outside controlled array index is used unchecked for data used as configuration for sound backend (alsa, oss, pulse, ...). The most likely outcome is a crash of the client instance followed by no or distorted sound or a session disconnect. If a user cannot upgrade to the patched version, a workaround is to disable sound for the session. This has been patched in 2.1.0.	2.2	More Details
CVE-2020-11040	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound data read from memory in clear_decompress_subcode_rlex, visualized on screen as color. This has been patched in 2.1.0.	2.2	More Details
CVE-2020-11043	In FreeRDP less than or equal to 2.0.0, there is an out-of-bounds read in rfx_process_message_tileset. Invalid data fed to RFX decoder results in garbage on screen (as colors). This has been patched in 2.1.0.	2.2	More Details
CVE-2019-5411	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5412	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5410	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12027	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12026	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12025	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12024	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12023	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12022	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12021	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12020	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12019	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12018	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12016	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12013	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12012	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12011	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12010	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12007	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12006	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12028	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12029	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12030	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5328	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5409	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5337	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5336	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5335	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5334	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5333	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5332	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5331	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5330	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5329	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5327	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12031	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-5324	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12040	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12039	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12038	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12037	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12036	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12035	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12034	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12033	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12032	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details
CVE-2019-12009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2019. Notes: none	N/A	More Details