SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 November 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-2020-27956	An Arbitrary File Upload in the Upload Image component in SourceCodester Car Rental Management System 1.0 allows the user to conduct remote code execution via admin/index.php?page=manage_car because .php files can be uploaded to admin/assets/uploads/ (under the web root).	9.8	More Details
CVE-2020-23639	A command injection vulnerability exists in Moxa Inc VPort 461 Series Firmware Version 3.4 or lower that could allow a remote attacker to execute arbitrary commands in Moxa's VPort 461 Series Industrial Video Servers.	9.8	More Details
CVE-2020-3673	u'Buffer overflow can happen as part of SIP message packet processing while storing values in array due to lack of check to validate the index length' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2020-3692	u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation for parameters received from server' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in Agatti, Kamorta, Nicobar, QCM6125, QCS610, Rennell, SA415M, Saipan, SC7180, SC8180X, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	9.8	More Details
CVE-2020-3703	u'Buffer over-read issue in Bluetooth peripheral firmware due to lack of check for invalid opcode and length of opcode received from central device(This CVE is equivalent to Link Layer Length Overfow issue (CVE-2019-16336,CVE-2019-17519) and Silent Length Overflow issue(CVE-2019-17518) mentioned in sweyntooth paper)' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8076, AR9344, Bitra, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, Nicobar, QCA6174A, QCA9377, QCM2150, QCM6125, QCS404, QCS405, QCS605, QCS610, QM215, Rennell, SC8180X, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	9.8	More Details
CVE-2018-19950	If exploited, this command injection vulnerability could allow remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Music Station versions prior to 5.1.13; versions prior to 5.2.9; versions prior to 5.3.11.	9.8	More Details
CVE-2018-17932	JUUKO K-800 (Firmware versions prior to numbers ending ...9A, ...9B, ...9C, etc.) is vulnerable to a replay attack and command forgery, which could allow attackers to replay commands, control the device, view commands, or cause the device to stop running.	9.8	More Details
CVE-2018-19025	In JUUKO K-808, an attacker could specially craft a packet that encodes an arbitrary command, which could be executed on the K-808 (Firmware versions prior to numbers ending ...9A, ...9B, ...9C, etc.).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14750	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2020-24881	SSRF exists in osTicket before 1.14.3, where an attacker can add malicious file to server or perform port scanning.	9.8	More Details
CVE-2020-3654	u'Buffer overflow occurs while processing SIP message packet due to lack of check of index validation before copying into it' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6390, QCA6574AU, QCM2150, QCS605, QM215, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	9.8	More Details
CVE-2020-28032	WordPress before 5.5.2 mishandles deserialization requests in wp-includes/Requests/Utility/FilteredIterator.php.	9.8	More Details
CVE-2020-28035	WordPress before 5.5.2 allows attackers to gain privileges via XML-RPC.	9.8	More Details
CVE-2020-28036	wp-includes/class-wp-xmlrpc-server.php in WordPress before 5.5.2 allows attackers to gain privileges by using XML-RPC to comment on a post.	9.8	More Details
CVE-2020-28037	is_blog_installed in wp-includes/functions.php in WordPress before 5.5.2 improperly determines whether WordPress is already installed, which might allow an attacker to perform a new installation, leading to remote code execution (as well as a denial of service for the old installation).	9.8	More Details
CVE-2020-5653	Buffer overflow vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	9.8	More Details
CVE-2020-5656	Improper access control vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet.	9.8	More Details
CVE-2020-15993	Use after free in printing in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	9.8	More Details
CVE-2020-8239	A vulnerability in the Pulse Secure Desktop Client < 9.1R9 is vulnerable to the client registry privilege escalation attack. This fix also requires Server Side Upgrade due to Standalone Host Checker Client (Windows) and Windows PDC.	9.8	More Details
CVE-2020-3657	u'Remote code execution can happen by sending a carefully crafted POST query when Device configuration is accessed from a tethered client through webserver due to lack of array bound check.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6574AU, QCS405, QCS610, QRB5165, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8250	9.8	More Details
CVE-2020-11172	u'fscanf reads a string from a file and stores its contents on a statically allocated stack memory which leads to stack overflow' in Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, QCA9531, QCA9980	9.8	More Details
CVE-2020-27654	Improper access control vulnerability in lbd in Synology Router Manager (SRM) before 1.2.4-8081 allows remote attackers to execute arbitrary commands via port (1) 7786/tcp or (2) 7787/tcp.	9.8	More Details
CVE-2020-27976	osCommerce Phoenix CE before 1.0.5.4 allows OS command injection remotely. Within admin/mail.php, a from POST parameter can be passed to the application. This affects the PHP mail function, and the sendmail -f option.	9.8	More Details
CVE-2020-16257	Winston 1.5.4 devices are vulnerable to command injection via the API.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-19949	If exploited, this command injection vulnerability could allow remote attackers to run arbitrary commands. QNAP has already fixed the issue in the following QTS versions. QTS 4.4.2.1231 on build 20200302; QTS 4.4.1.1201 on build 20200130; QTS 4.3.6.1218 on build 20200214; QTS 4.3.4.1190 on build 20200107; QTS 4.3.3.1161 on build 20200109; QTS 4.2.6 on build 20200109.	9.8	More Details
CVE-2020-16259	Winston 1.5.4 devices have an SSH user account with access from bastion hosts. This is undocumented in device documents and is not announced to the user.	9.8	More Details
CVE-2020-27739	A Weak Session Management vulnerability in Citadel WebCit through 926 allows unauthenticated remote attackers to hijack recently logged-in users' sessions. NOTE: this was reported to the vendor in a publicly archived "Multiple Security Vulnerabilities in WebCit 926" thread.	9.8	More Details
CVE-2020-11483	NVIDIA DGX servers, all DGX-1 with BMC firmware versions prior to 3.38.30 and all DGX-2 with BMC firmware versions prior to 1.06.06, contains a vulnerability in the AMI BMC firmware in which the firmware includes hard-coded credentials, which may lead to elevation of privileges or information disclosure.	9.8	More Details
CVE-2020-11486	NVIDIA DGX servers, all DGX-1 with BMC firmware versions prior to 3.38.30, contain a vulnerability in the AMI BMC firmware in which software allows an attacker to upload or transfer files that can be automatically processed within the product's environment, which may lead to remote code execution.	9.8	More Details
CVE-2020-27744	An issue was discovered on Western Digital My Cloud NAS devices before 5.04.114. They allow remote code execution with resultant escalation of privileges.	9.8	More Details
CVE-2020-27995	SQL Injection in Zoho ManageEngine Applications Manager 14 before 14560 allows an attacker to execute commands on the server via the MyPage.do template_resid parameter.	9.8	More Details
CVE-2020-27998	An issue was discovered in FastReport before 2020.4.0. It lacks a ScriptSecurity feature and therefore may mishandle (for example) GetType, typeof, TypeOf, DllImport, LoadLibrary, and GetProcAddress.	9.8	More Details
CVE-2020-27886	An issue was discovered in EyesOfNetwork eonweb 5.3-7 through 5.3-8. The eonweb web interface is prone to a SQL injection, allowing an unauthenticated attacker to exploit the username_available function of the includes/functions.php file (which is called by login.php).	9.8	More Details
CVE-2020-7373	vBulletin 5.5.4 through 5.6.2 allows remote command execution via crafted subWidgets data in an ajax/render/widget_tabbedcontainer_tab_panel request. NOTE: this issue exists because of an incomplete fix for CVE-2019-16759. ALSO NOTE: CVE-2020-7373 is a duplicate of CVE-2020-17496. CVE-2020-17496 is the preferred CVE ID to track this vulnerability.	9.8	More Details
CVE-2020-11153	u'Out of bound memory access while processing GATT data received due to lack of check of pdu data length and leads to remote code execution' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8053, QCA6390, QCA9379, QCN7605, SC8180X, SDX55	9.8	More Details
CVE-2020-1909	A use-after-free in a logging library in WhatsApp for iOS prior to v2.20.111 and WhatsApp Business for iOS prior to v2.20.111 could have resulted in memory corruption, crashes and potentially code execution. This could have happened only if several events occurred together in sequence, including receiving an animated sticker while placing a WhatsApp video call on hold.	9.8	More Details
CVE-2020-16011	Heap buffer overflow in UI in Google Chrome on Windows prior to 86.0.4240.183 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2020-3670	u'Potential out of bounds read while processing downlink NAS transport message due to improper length check of Information Element(IEI) NAS message container' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909W, MSM8917, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCM6125, QCS605, QCS610, QM215, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	9.1	More Details
CVE-2020-16263	Winston 1.5.4 devices have a CORS configuration that trusts arbitrary origins. This allows requests to be made and viewed by arbitrary origins.	9.1	More Details
CVE-2020-28039	is_protected_meta in wp-includes/meta.php in WordPress before 5.5.2 allows arbitrary file deletion because it does not properly determine whether a meta key is considered protected.	9.1	More Details
CVE-2020-11169	u'Buffer over-read while processing received L2CAP packet due to lack of integer overflow check' in Snapdragon Auto, 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 APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-15975	Integer overflow in SwiftShader in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16256	The API on Winston 1.5.4 devices is vulnerable to CSRF.	8.8	More Details
CVE-2020-15994	Use after free in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15992	Insufficient policy enforcement in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page.	8.8	More Details
CVE-2020-15991	Use after free in password manager in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-15990	Use after free in autofill in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-15987	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC stream.	8.8	More Details
CVE-2020-15979	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15978	Insufficient data validation in navigation in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	8.8	More Details
CVE-2020-15976	Use after free in WebXR in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-27996	An issue was discovered in SmartStoreNET before 4.0.1. It does not properly consider the need for a CustomModelPartAttribute decoration in certain ModelBase.CustomProperties situations.	8.8	More Details
CVE-2020-15974	Integer overflow in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.	8.8	More Details
CVE-2020-15972	Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15971	Use after free in printing in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-15970	Use after free in NFC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-15969	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15968	Use after free in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15967	Use after free in payments in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-11485	NVIDIA DGX servers, all DGX-1 with BMC firmware versions prior to 3.38.30, contains a Cross-Site Request Forgery (CSRF) vulnerability in the AMI BMC firmware in which the web application does not sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, which can lead to information disclosure or code execution.	8.8	More Details
CVE-2020-11155	u'Buffer overflow while processing PDU packet in bluetooth due to lack of check of buffer length before copying into it.' in Snapdragon Auto, 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 APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	8.8	More Details
CVE-2020-11154	u'Buffer overflow while processing a crafted PDU data packet in bluetooth due to lack of check of buffer size before copying' in Snapdragon Auto, 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 APQ8009, APQ8053, QCA6390, QCN7605, QCN7606, SA415M, SA515M, SA6155P, SA8155P, SC8180X, SDX55	8.8	More Details
CVE-2020-11114	u'Bluetooth devices does not properly restrict the L2CAP payload length allowing users in radio range to cause a buffer overflow via a crafted Link Layer packet(Equivalent to CVE-2019-17060,CVE-2019-17061 and CVE-2019-17517 in Sweyntooth paper)' in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in AR9344	8.8	More Details
CVE-2020-25849	MailGates and MailAudit products contain Command Injection flaw, which can be used to inject and execute system commands from the cgi parameter after attackers obtain the user's access token.	8.8	More Details
CVE-2020-15995	Out of bounds write in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-27887	An issue was discovered in EyesOfNetwork 5.3 through 5.3-8. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the nmap_binary parameter to lilac/autodiscovery.php.	8.8	More Details
CVE-2020-15996	Use after free in passwords in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-27975	osCommerce Phoenix CE before 1.0.5.4 allows admin/define_language.php CSRF.	8.8	More Details
CVE-2020-16010	Heap buffer overflow in UI in Google Chrome on Android prior to 86.0.4240.185 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-8254	A vulnerability in the Pulse Secure Desktop Client < 9.1R9 has Remote Code Execution (RCE) if users can be convinced to connect to a malicious server. This vulnerability only affects Windows PDC.To improve the security of connections between Pulse clients and Pulse Connect Secure, see below recommendation(s):Disable Dynamic certificate trust for PDC.	8.8	More Details
CVE-2020-16009	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16008	Stack buffer overflow in WebRTC in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit stack corruption via a crafted WebRTC packet.	8.8	More Details
CVE-2020-16005	Insufficient policy enforcement in ANGLE in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16004	Use after free in user interface in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16003	Use after free in printing in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16002	Use after free in PDFium in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	8.8	More Details
CVE-2020-16006	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-16001	Use after free in media in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-15997	Use after free in Mojo in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-15998	Use after free in USB in Google Chrome prior to 86.0.4240.99 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	8.8	More Details
CVE-2020-16000	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-5145	SonicWall Global VPN client version 4.10.4.0314 and earlier have an insecure library loading (DLL hijacking) vulnerability. Successful exploitation could lead to remote code execution in the target system.	8.6	More Details
CVE-2020-27652	Algorithm downgrade vulnerability in QuickConnect in Synology DiskStation Manager (DSM) before 6.2.3-25426-2 allows man-in-the-middle attackers to spoof servers and obtain sensitive information via unspecified vectors.	8.3	More Details
CVE-2020-27649	Improper certificate validation vulnerability in OpenVPN client in Synology Router Manager (SRM) before 1.2.4-8081 allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	8.3	More Details
CVE-2020-27648	Improper certificate validation vulnerability in OpenVPN client in Synology DiskStation Manager (DSM) before 6.2.3-25426-2 allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	8.3	More Details
CVE-2020-27653	Algorithm downgrade vulnerability in QuickConnect in Synology Router Manager (SRM) before 1.2.4-8081 allows man-in-the-middle attackers to spoof servers and obtain sensitive information via unspecified vectors.	8.3	More Details
CVE-2020-11141	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap configuration request received from peer device.' in Snapdragon Auto, 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 APQ8009, APQ8053, QCA6390, QCN7605, SA415M, SA515M, SC8180X, SDX55, SM8250	8.1	More Details
CVE-2020-11156	u'Buffer over-read issue in Bluetooth estack due to lack of check for invalid length of L2cap packet received from peer device.' in Snapdragon Auto, 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 QCA6390, QCN7605, QCS404, SA415M, SA515M, SC8180X, SDX55, SM8250	8.1	More Details
CVE-2018-19943	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code. QNAP has already fixed these issues in the following QTS versions. QTS 4.4.2.1270 build 20200410 and later QTS 4.4.1.1261 build 20200330 and later QTS 4.3.6.1263 build 20200330 and later QTS 4.3.4.1282 build 20200408 and later QTS 4.3.3.1252 build 20200409 and later QTS 4.2.6 build 20200421 and later	8.0	More Details
CVE-2020-5425	Single Sign-On for Vmware Tanzu all versions prior to 1.11.3 ,1.12.x versions prior to 1.12.4 and 1.13.x prior to 1.13.1 are vulnerable to user impersonation attack.If two users are logged in to the SSO operator dashboard at the same time, with the same username, from two different identity providers, one can acquire the token of the other and thus operate with their permissions. Note: Foundation may be vulnerable only if: 1) The system zone is set up to use a SAML identity provider 2) There are internal users that have the same username as users in the external SAML provider 3) Those duplicate-named users have the scope to access the SSO operator dashboard 4) The vulnerability doesn't appear with LDAP because of chained authentication.	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11174	u'Array index underflow issue in adsp driver due to improper check of channel id before used as array index.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8953, MSM8996AU, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-3684	u'QSEE reads the access permission policy for the SMEM TOC partition from the SMEM TOC contents populated by XBL Loader and applies them without 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 Agatti, APQ8009, APQ8098, Bitra, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8998, Nicobar, QCA6390, QCS404, QCS405, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-4722	IBM i2 Analyst Notebook 9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 187870.	7.8	More Details
CVE-2020-4724	IBM i2 Analyst Notebook 9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.	7.8	More Details
CVE-2020-3678	u'A buffer overflow could occur if the API is improperly used due to UIE init does not contain a buffer size a param' in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Kamorta, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SXR1130	7.8	More Details
CVE-2020-3638	u'An Unaligned address or size can propagate to the database due to improper page permissions and can lead to improper access control' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, QCA6390, QCS404, QCS610, Rennell, SA515M, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-5144	SonicWall Global VPN client version 4.10.4.0314 and earlier allows unprivileged windows user to elevate privileges to SYSTEM through loaded process hijacking vulnerability.	7.8	More Details
CVE-2020-5991	NVIDIA CUDA Toolkit, all versions prior to 11.1.1, contains a vulnerability in the NVJPEG library in which an out-of-bounds read or write operation may lead to code execution, denial of service, or information disclosure.	7.8	More Details
CVE-2020-11162	u'Possible buffer overflow in MHI driver due to lack of input parameter validation of EOT events received from MHI device side' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8917, MSM8953, Nicobar, QCA6390, QCM2150, QCS404, QCS405, QCS605, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-4721	IBM i2 Analyst Notebook 9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 187868.	7.8	More Details
CVE-2020-8240	A vulnerability in the Pulse Secure Desktop Client < 9.1R9 allows a restricted user on an endpoint machine can use system-level privileges if the Embedded Browser is configured with Credential Provider. This vulnerability only affects Windows PDC if the Embedded Browser is configured with the Credential Provider.	7.8	More Details
CVE-2020-4723	IBM i2 Analyst Notebook 9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 187873.	7.8	More Details
CVE-2020-4588	IBM i2 iBase 8.9.13 could allow an attacker to upload arbitrary executable files which, when executed by an unsuspecting victim could result in code execution. IBM X-Force ID: 184579.	7.8	More Details
CVE-2020-11164	u'Third-party app may also call the broadcasts in Perfdump and cause privilege escalation issue due to improper access control' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in Agatti, APQ8096AU, APQ8098, Bitra, Kamorta, MSM8909W, MSM8917, MSM8940, Nicobar, QCA6390, QCM2150, QCS605, Rennell, SA6155P, SA8155P, Saipan, SDA660, SDM429W, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14425	Foxit Reader before 10.0 allows Remote Command Execution via the app.opencPDFWebPage JavsScript API. An attacker can execute local files and bypass the security dialog.	7.8	More Details
CVE-2020-3690	u'Due to an incorrect SMMU configuration, the modem crypto engine can potentially compromise the hypervisor' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Agatti, Bitra, Kamorta, Nicobar, QCA6390, QCS404, QCS605, QCS610, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-3693	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-16262	Winston 1.5.4 devices have a local www-data user that is overly permissioned, resulting in root privilege escalation.	7.8	More Details
CVE-2020-26130	Issues were discovered in Open TFTP Server multithreaded 1.66 and Open TFTP Server single port 1.66. Due to insufficient access restrictions in the default installation directory, an attacker can elevate privileges by replacing the OpenTFTPServerMT.exe or the OpenTFTPServerSP.exe binary.	7.8	More Details
CVE-2020-26131	Issues were discovered in Open DHCP Server (Regular) 1.75 and Open DHCP Server (LDAP Based) 0.1Beta. Due to insufficient access restrictions in the default installation directory, an attacker can elevate privileges by replacing the OpenDHCPServer.exe (Regular) or the OpenDHCPLdap.exe (LDAP Based) binary.	7.8	More Details
CVE-2020-26132	An issue was discovered in Home DNS Server 0.10. Due to insufficient access restrictions in the default installation directory, an attacker can elevate privileges by replacing the HomeDNSServer.exe binary.	7.8	More Details
CVE-2020-26133	An issue was discovered in Dual DHCP DNS Server 7.40. Due to insufficient access restrictions in the default installation directory, an attacker can elevate privileges by replacing the DualServer.exe binary.	7.8	More Details
CVE-2020-15983	Insufficient data validation in webUI in Google Chrome on ChromeOS prior to 86.0.4240.75 allowed a local attacker to bypass content security policy via a crafted HTML page.	7.8	More Details
CVE-2020-15980	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to bypass navigation restrictions via crafted Intents.	7.8	More Details
CVE-2020-24707	Gophish before 0.11.0 allows the creation of CSV sheets that contain malicious content.	7.8	More Details
CVE-2020-16007	Insufficient data validation in installer in Google Chrome prior to 86.0.4240.183 allowed a local attacker to potentially elevate privilege via a crafted filesystem.	7.8	More Details
CVE-2020-8250	A vulnerability in the Pulse Secure Desktop Client (Linux) < 9.1R9 could allow local attackers to escalate privilege.	7.8	More Details
CVE-2020-8249	A vulnerability in the Pulse Secure Desktop Client (Linux) < 9.1R9 could allow local attackers to perform buffer overflow.	7.8	More Details
CVE-2020-28046	An issue was discovered in ProlinOS through 2.4.161.8859R. An attacker with local code execution privileges as a normal user (MAINAPP) can escalate to root privileges by exploiting the setuid installation of the xtables-multi binary and leveraging the ip6tables --modprobe switch.	7.8	More Details
CVE-2020-8248	A vulnerability in the Pulse Secure Desktop Client (Linux) < 9.1R9 could allow local attackers to escalate privilege.	7.8	More Details
CVE-2020-28045	An unsigned-library issue was discovered in ProlinOS through 2.4.161.8859R. This OS requires installed applications and all system binaries to be signed either by the manufacturer or by the Point Of Sale application developer and distributor. The signature is a 2048-byte RSA signature verified in the kernel prior to ELF execution. Shared libraries, however, do not need to be signed, and they are not verified. An attacker may execute a custom binary by compiling it as a shared object and loading it via LD_PRELOAD.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27992	Dr.Fone 3.0.0 allows local users to gain privileges via a Trojan horse DriverInstall.exe because %PROGRAMFILES(X86)%\Wondershare\dr.fone\Library\DriverInstaller has Full Control for BUILTIN\Users.	7.8	More Details
CVE-2020-27708	A vulnerability exists in the Origin Client that could allow a non-Administrative user to elevate their access to either Administrator or System. Once the user has obtained elevated access, they may be able to take control of the system and perform actions otherwise reserved for high privileged users or system Administrators.	7.8	More Details
CVE-2020-3696	u'Use after free while installing new security rule in ipcrtr as old one is deleted and this rule could still be in use for checking security permission for particular process' in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial 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, MSM8905, MSM8909W, MSM8996AU, QCA4531, QCA6574AU, QCA9531, QCM2150, QCS605, SDM429W, SDX20, SDX24	7.8	More Details
CVE-2020-3694	u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom' in Snapdragon Auto, Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in Bitra, Nicobar, Saipan, SM6150, SM8150, SM8250, SXR2130	7.8	More Details
CVE-2020-11125	u'Out of bound access can happen in MHI command process due to lack of check of channel id value received from MHI devices' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8009, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9150, MDM9607, MDM9650, MSM8905, MSM8917, MSM8953, Nicobar, QCA6390, QCA9531, QCM2150, QCS404, QCS405, QCS605, QCS610, QM215, QRB5165, Rennell, SA415M, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM660, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.8	More Details
CVE-2020-26210	In BookStack before version 0.30.4, a user with permissions to edit a page could add an attached link which would execute untrusted JavaScript code when clicked by a viewer of the page. Dangerous content may remain in the database after this update. If you think this could have been exploited the linked advisory provides a SQL query to test. As a workaround, page edit permissions could be limited to only those that are trusted until you can upgrade although this will not address existing exploitation of this vulnerability. The issue is fixed in version 0.30.4.	7.7	More Details
CVE-2020-15276	baserCMS before version 4.4.1 is vulnerable to Cross-Site Scripting. Arbitrary JavaScript may be executed by entering a crafted nickname in blog comments. The issue affects the blog comment component. It is fixed in version 4.4.1.	7.7	More Details
CVE-2020-26211	In BookStack before version 0.30.4, a user with permissions to edit a page could insert JavaScript code through the use of `javascript:` URIs within a link or form which would run, within the context of the current page, when clicked or submitted. Additionally, a user with permissions to edit a page could insert a particular meta tag which could be used to silently redirect users to a alternative location upon visit of a page. Dangerous content may remain in the database but will be removed before being displayed on a page. If you think this could have been exploited the linked advisory provides a SQL query to test. As a workaround without upgrading, page edit permissions could be limited to only those that are trusted until you can upgrade although this will not address existing exploitation of this vulnerability. The issue is fixed in BookStack version 0.30.4.	7.7	More Details
CVE-2020-15278	Red Discord Bot before version 3.4.1 has an unauthorized privilege escalation exploit in the Mod module. This exploit allows Discord users with a high privilege level within the guild to bypass hierarchy checks when the application is in a specific condition that is beyond that user's control. By abusing this exploit, it is possible to perform destructive actions within the guild the user has high privileges in. This exploit has been fixed in version 3.4.1. As a workaround, unloading the Mod module with unload mod or, disabling the massban command with command disable global massban can render this exploit not accessible. We still highly recommend updating to 3.4.1 to completely patch this issue.	7.7	More Details
CVE-2020-26205	Sal is a multi-tenanted reporting dashboard for Munki with the ability to display information from Facter. In Sal through version 4.1.6 there is an XSS vulnerability on the machine_list view.	7.6	More Details
CVE-2020-11487	NVIDIA DGX servers, DGX-1 with BMC firmware versions prior to 3.38.30. DGX-2 with BMC firmware versions prior to 1.06.06 and all DGX A100 Servers with all BMC firmware versions, contains a vulnerability in the AMI BMC firmware in which the use of a hard-coded RSA 1024 key with weak ciphers may lead to information disclosure.	7.5	More Details
CVE-2020-3704	u'While processing invalid connection request PDU which is nonstandard (interval or timeout is 0) from central device may lead peripheral system enter into dead lock state.(This CVE is equivalent to InvalidConnectionRequest(CVE-2019-19193) mentioned in sweyntooth paper)' 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 Wired Infrastructure and Networking in Agatti, APQ8009, APQ8017, APQ8053, AR9344, Bitra, IPQ5018, Kamorta, MDM9607, MDM9640, MDM9650, MSM8996AU, Nicobar, QCA6174A, QCA6390, QCA6574AU, QCA9377, QCA9886, QCM6125, QCN7605, QCS404, QCS405, QCS605, QCS610, QRB5165, Rennell, SA415M, SA515M, Saipan, SC7180, SC8180X, SDA845, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-19952	If exploited, this SQL injection vulnerability could allow remote attackers to obtain application information. This issue affects: QNAP Systems Inc. Music Station versions prior to 5.1.13; versions prior to 5.2.9; versions prior to 5.3.11.	7.5	More Details
CVE-2020-10937	An issue was discovered in IPFS (aka go-ipfs) 0.4.23. An attacker can generate ephemeral identities (Sybils) and leverage the IPFS connection management reputation system to poison other nodes' routing tables, eclipsing the nodes that are the target of the attack from the rest of the network. Later versions, in particular go-ipfs 0.7, mitigate this.	7.5	More Details
CVE-2020-11615	NVIDIA DGX servers, all BMC firmware versions prior to 3.38.30, contain a vulnerability in the AMI BMC firmware in which it uses a hard-coded RC4 cipher key, which may lead to information disclosure.	7.5	More Details
CVE-2020-27978	Shibboleth Identify Provider 3.x before 3.4.6 has a denial of service flaw. A remote unauthenticated attacker can cause a login flow to trigger Java heap exhaustion due to the creation of objects in the Java Servlet container session.	7.5	More Details
CVE-2020-4767	IBM Sterling Connect Direct for Microsoft Windows 4.7, 4.8, 6.0, and 6.1 could allow a remote attacker to cause a denial of service, caused by a buffer over-read. Bysending a specially crafted request, the attacker could cause the application to crash. IBM X-Force ID: 188906.	7.5	More Details
CVE-2020-11489	NVIDIA DGX servers, all DGX-1 with BMC firmware versions prior to 3.38.30 and all DGX-2 with BMC firmware versions prior to 1.06.06, contain a vulnerability in the AMI BMC firmware in which default SNMP community strings are used, which may lead to information disclosure.	7.5	More Details
CVE-2020-28030	In Wireshark 3.2.0 to 3.2.7, the GQUIC dissector could crash. This was addressed in epan/dissectors/packet-gquic.c by correcting the implementation of offset advancement.	7.5	More Details
CVE-2020-28033	WordPress before 5.5.2 mishandles embeds from disabled sites on a multisite network, as demonstrated by allowing a spam embed.	7.5	More Details
CVE-2020-16260	Winston 1.5.4 devices do not enforce authorization. This is exploitable from the intranet, and can be combined with other vulnerabilities for remote exploitation.	7.5	More Details
CVE-2020-28043	MISP through 2.4.133 allows SSRF in the REST client via the use_full_path parameter with an arbitrary URL.	7.5	More Details
CVE-2020-5652	Uncontrolled resource consumption vulnerability in Ethernet Port on MELSEC iQ-R, Q and L series CPU modules (R 00/01/02 CPU firmware versions '20' and earlier, R 04/08/16/32/120 (EN) CPU firmware versions '52' and earlier, R 08/16/32/120 SFCPU firmware versions '22' and earlier, R 08/16/32/120 PCPU all versions, R 08/16/32/120 PSFCPU all versions, R 16/32/64 MTCPU all versions, Q03 UDECPU, Q 04/06/10/13/20/26/50/100 UDEHCPU serial number '22081' and earlier , Q 03/04/06/13/26 UDVCPU serial number '22031' and earlier, Q 04/06/13/26 UDPVCPU serial number '22031' and earlier, Q 172/173 DCPU all versions, Q 172/173 DSCPU all versions, Q 170 MCPU all versions, Q 170 MSCPU all versions, L 02/06/26 CPU (-P) and L 26 CPU - (P) BT all versions) allows a remote unauthenticated attacker to stop the Ethernet communication functions of the products via a specially crafted packet, which may lead to a denial of service (DoS) condition .	7.5	More Details
CVE-2020-7746	This affects the package chart.js before 2.9.4. The options parameter is not properly sanitized when it is processed. When the options are processed, the existing options (or the defaults options) are deeply merged with provided options. However, during this operation, the keys of the object being set are not checked, leading to a prototype pollution.	7.5	More Details
CVE-2020-5654	Session fixation vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.	7.5	More Details
CVE-2020-5655	NULL pointer dereferences vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5658	Resource Management Errors vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows a remote unauthenticated attacker to stop the network functions of the products via a specially crafted packet.	7.5	More Details
CVE-2020-8183	A logic error in Nextcloud Server 19.0.0 caused a plaintext storage of the share password when it was given on the initial create API call.	7.5	More Details
CVE-2020-9368	The Module Olea Gift On Order module through 5.0.8 for PrestaShop enables an unauthenticated user to read arbitrary files on the server via getfile.php?file=/.. directory traversal.	7.5	More Details
CVE-2020-25966	Sectona Spectra before 3.4.0 has a vulnerable SOAP API endpoint that leaks sensitive information about the configured assets without proper authentication. This could be used by unauthorized parties to get configured login credentials of the assets via a modified pAccountID value. NOTE: The vendor has indicated this is not a vulnerability and states "This vulnerability occurred due to wrong configuration of system.	7.5	More Details
CVE-2020-24990	An issue was discovered in QSC Q-SYS Core Manager 8.2.1. By utilizing the TFTP service running on UDP port 69, a remote attacker can perform a directory traversal and obtain operating system files via a TFTP GET request, as demonstrated by reading /etc/passwd or /proc/version.	7.5	More Details
CVE-2020-7758	This affects versions of package browserless-chrome before 1.40.2-chrome-stable. User input flowing from the workspace endpoint gets used to create a file path filePath and this is fetched and then sent back to a user. This can be escaped to fetch arbitrary files from a server.	7.5	More Details
CVE-2020-9861	A stack overflow issue existed in Swift for Linux. The issue was addressed with improved input validation for dealing with deeply nested malicious JSON input.	7.5	More Details
CVE-2020-27986	SonarQube 8.4.2.36762 allows remote attackers to discover cleartext SMTP, SVN, and GitLab credentials via the api/settings/values URI. NOTE: reportedly, the vendor's position for SMTP and SVN is "it is the administrator's responsibility to configure it.	7.5	More Details
CVE-2020-24713	Gophish through 0.10.1 does not invalidate the gophish cookie upon logout.	7.5	More Details
CVE-2020-11616	NVIDIA DGX servers, all BMC firmware versions prior to 3.38.30, contain a vulnerability in the AMI BMC firmware in which the Pseudo-Random Number Generator (PRNG) algorithm used in the JSOL package that implements the IPMI protocol is not cryptographically strong, which may lead to information disclosure.	7.5	More Details
CVE-2020-25780	In CommCell in Commvault before 14.68, 15.x before 15.58, 16.x before 16.44, 17.x before 17.29, and 18.x before 18.13, Directory Traversal can occur such that an attempt to view a log file can instead view a file outside of the log-files folder.	7.5	More Details
CVE-2020-8241	A vulnerability in the Pulse Secure Desktop Client < 9.1R9 could allow the attacker to perform a MITM Attack if end users are convinced to connect to a malicious server.	7.5	More Details
CVE-2020-11157	u'Lack of handling unexpected control messages while encryption was in progress can terminate the connection and thus leading to a DoS' in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8076, MDM9640, MDM9650, MSM8905, MSM8917, MSM8937, MSM8940, MSM8953, QCA6174A, QCA9886, QCM2150, QM215, SDM429, SDM439, SDM450, SDM632	7.5	More Details
CVE-2020-5931	On BIG-IP 15.1.0-15.1.0.5, 14.1.0-14.1.2.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, Virtual servers with a OneConnect profile may incorrectly handle WebSockets related HTTP response headers, causing TMM to restart.	7.5	More Details
CVE-2020-4584	IBM i2 iBase 8.9.13 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: 184574.	7.5	More Details
CVE-2020-22552	The Snap7 server component in version 1.4.1, when an attacker sends a crafted packet with COTP protocol the last-data-unit flag set to No and S7 writes a var function, the Snap7 server will be crashed.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25646	A flaw was found in Ansible Collection community.crypto. openssl_privatekey_info exposes private key in logs. This directly impacts confidentiality	7.5	More Details
CVE-2020-5936	On BIG-IP LTM 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, and 12.1.0-12.1.5.1, the Traffic Management Microkernel (TMM) process may consume excessive resources when processing SSL traffic and client authentication are enabled on the client SSL profile.	7.5	More Details
CVE-2020-5937	On BIG-IP AFM 15.1.0-15.1.0.5, the Traffic Management Microkernel (TMM) may produce a core file while processing layer 4 (L4) behavioral denial-of-service (DoS) traffic.	7.5	More Details
CVE-2020-5933	On versions 15.1.0-15.1.0.5, 14.1.0-14.1.2.3, 13.1.0-13.1.3.4, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, when a BIG-IP system that has a virtual server configured with an HTTP compression profile processes compressed HTTP message payloads that require deflation, a Slowloris-style attack can trigger an out-of-memory condition on the BIG-IP system.	7.5	More Details
CVE-2020-15273	baserCMS before version 4.4.1 is vulnerable to Cross-Site Scripting. The issue affects the following components: Edit feed settings, Edit widget area, Sub site new registration, New category registration. Arbitrary JavaScript may be executed by entering specific characters in the account that can access the file upload function category list, subsite setting list, widget area edit, and feed list on the management screen. The issue was introduced in version 4.0.0. It is fixed in version 4.4.1.	7.3	More Details
CVE-2020-15277	baserCMS before version 4.4.1 is affected by Remote Code Execution (RCE). Code may be executed by logging in as a system administrator and uploading an executable script file such as a PHP file. The Edit template component is vulnerable. The issue is fixed in version 4.4.1.	7.2	More Details
CVE-2020-8260	A vulnerability in the Pulse Connect Secure < 9.1R9 admin web interface could allow an authenticated attacker to perform an arbitrary code execution using uncontrolled gzip extraction.	7.2	More Details
CVE-2020-16258	Winston 1.5.4 devices make use of a Monit service (not managed during the normal user process) which is configured with default credentials.	7.1	More Details
CVE-2020-27658	Synology Router Manager (SRM) before 1.2.4-8081 does not include the HTTPOnly flag in a Set-Cookie header for the session cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie.	7.1	More Details
CVE-2020-11173	u'Two threads running simultaneously from user space can lead to race condition in fastRPC driver' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in Agatti, APQ8053, Bitra, IPQ4019, IPQ5018, IPQ6018, IPQ8064, IPQ8074, Kamorta, MDM9607, MSM8953, Nicobar, QCA6390, QCS404, QCS405, QCS610, Rennell, SA515M, SA6155P, SA8155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM632, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	7.0	More Details
CVE-2020-7384	Rapid7's Metasploit msfvenom framework handles APK files in a way that allows for a malicious user to craft and publish a file that would execute arbitrary commands on a victim's machine.	7.0	More Details
CVE-2020-8236	A wrong configuration in Nextcloud Server 19.0.1 incorrectly made the user feel the passwordless WebAuthn is also a two factor verification by asking for the PIN of the passwordless WebAuthn but not verifying it.	6.8	More Details
CVE-2020-27747	An issue was discovered in Click Studios Passwordstate 8.9 (Build 8973).If the user of the system has assigned himself a PIN code for entering from a mobile device using the built-in generator (4 digits), a remote attacker has the opportunity to conduct a brute force attack on this PIN code. As result, remote attacker retrieves all passwords from another systems, available for affected account.	6.8	More Details
CVE-2020-28044	An attacker with physical access to a PAX Point Of Sale device with ProlinOS through 2.4.161.8859R can boot it in management mode, enable the XCB service, and then list, read, create, and overwrite files with MAINAPP permissions.	6.8	More Details
CVE-2020-16261	Winston 1.5.4 devices allow a U-Boot interrupt, resulting in local root access.	6.8	More Details
CVE-2020-11488	NVIDIA DGX servers, all DGX-1 with BMC firmware versions prior to 3.38.30 and all DGX-2 with BMC firmware versions prior to 1.06.06, contains a vulnerability in the AMI BMC firmware in which software does not validate the RSA 1024 public key used to verify the firmware signature, which may lead to information disclosure or code execution.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5934	On BIG-IP APM 15.1.0-15.1.0.5, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when multiple HTTP requests from the same client to configured SAML Single Logout (SLO) URL are passing through a TCP Keep-Alive connection, traffic to TMM can be disrupted.	6.5	More Details
CVE-2020-15981	Out of bounds read in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2020-15973	Insufficient policy enforcement in extensions in Google Chrome prior to 86.0.4240.75 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension.	6.5	More Details
CVE-2020-5657	Improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability in TCP/IP function included in the firmware of MELSEC iQ-R series (RJ71EIP91 EtherNet/IP Network Interface Module First 2 digits of serial number are '02' or before, RJ71PN92 PROFINET IO Controller Module First 2 digits of serial number are '01' or before, RD81DL96 High Speed Data Logger Module First 2 digits of serial number are '08' or before, RD81MES96N MES Interface Module First 2 digits of serial number are '04' or before, and RD81OPC96 OPC UA Server Module First 2 digits of serial number are '04' or before) allows unauthenticated attackers on adjacent network to stop the network functions of the products via a specially crafted packet.	6.5	More Details
CVE-2020-15985	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to spoof security UI via a crafted HTML page.	6.5	More Details
CVE-2020-6014	Check Point Endpoint Security Client for Windows, with Anti-Bot or Threat Emulation blades installed, before version E83.20, tries to load a non-existent DLL during a query for the Domain Name. An attacker with administrator privileges can leverage this to gain code execution within a Check Point Software Technologies signed binary, where under certain circumstances may cause the client to terminate.	6.5	More Details
CVE-2020-7759	The package pimcore/pimcore from 6.7.2 and before 6.8.3 are vulnerable to SQL Injection in data classification functionality in ClassificationstoreController. This can be exploited by sending a specifically-crafted input in the relationIds parameter as demonstrated by the following request: http://vulnerable.pimcore.example/admin/classificationstore/relations?relationIds=[{"keyId"%3a"'"","groupId"%3a"'asd'))+or+1%3d1+union+(select+1,2,3,4,5,6,name,8,password,",11,12,",14+from+users)+--+"}]	6.5	More Details
CVE-2020-15977	Insufficient data validation in dialogs in Google Chrome on OS X prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.	6.5	More Details
CVE-2020-7757	This affects all versions of package droppy. It is possible to traverse directories to fetch configuration files from a droopy server.	6.5	More Details
CVE-2020-15982	Inappropriate implementation in cache in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2020-15984	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 86.0.4240.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted URL.	6.5	More Details
CVE-2020-15986	Integer overflow in media in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2020-24711	The Reset button on the Account Settings page in Gophish before 0.11.0 allows attackers to cause a denial of service via a clickjacking attack	6.5	More Details
CVE-2020-6557	Inappropriate implementation in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	6.5	More Details
CVE-2020-27742	An Insecure Direct Object Reference vulnerability in Citadel WebCit through 926 allows authenticated remote attackers to read someone else's emails via the msg_confirm_move template. NOTE: this was reported to the vendor in a publicly archived "Multiple Security Vulnerabilities in WebCit 926" thread.	6.5	More Details
CVE-2020-28041	The SIP ALG implementation on NETGEAR Nighthawk R7000 1.0.9.64_10.2.64 devices allows remote attackers to communicate with arbitrary TCP and UDP services on a victim's intranet machine, if the victim visits an attacker-controlled web site with a modern browser, aka NAT Slipstreaming. This occurs because the ALG takes action based on an IP packet with an initial REGISTER substring in the TCP data, and the correct intranet IP address in the subsequent Via header, without properly considering that connection progress and fragmentation affect the meaning of the packet data.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27657	Cleartext transmission of sensitive information vulnerability in DDNS in Synology Router Manager (SRM) before 1.2.4-8081 allows man-in-the-middle attackers to eavesdrop authentication information of DNSExit via unspecified vectors.	6.5	More Details
CVE-2020-27656	Cleartext transmission of sensitive information vulnerability in DDNS in Synology DiskStation Manager (DSM) before 6.2.3-25426-2 allows man-in-the-middle attackers to eavesdrop authentication information of DNSExit via unspecified vectors.	6.5	More Details
CVE-2020-4782	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	6.5	More Details
CVE-2020-27655	Improper access control vulnerability in Synology Router Manager (SRM) before 1.2.4-8081 allows remote attackers to access restricted resources via inbound QuickConnect traffic.	6.5	More Details
CVE-2020-15999	Heap buffer overflow in Freetype in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2020-5938	On BIG-IP 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, when negotiating IPSec tunnels with configured, authenticated peers, the peer may negotiate a different key length than the BIG-IP configuration would otherwise allow.	6.5	More Details
CVE-2020-27014	Trend Micro Antivirus for Mac 2020 (Consumer) contains a race condition vulnerability in the Web Threat Protection Blocklist component, that if exploited, could allow an attacker to case a kernel panic or crash.\n\n\r\nAn attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability.	6.4	More Details
CVE-2020-15988	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 86.0.4240.75 allowed a remote attacker who convinced the user to open files to execute arbitrary code via a crafted HTML page.	6.3	More Details
CVE-2020-28038	WordPress before 5.5.2 allows stored XSS via post slugs.	6.1	More Details
CVE-2020-21266	Broadleaf Commerce 5.1.14-GA is affected by cross-site scripting (XSS) due to a slow HTTP post vulnerability.	6.1	More Details
CVE-2018-19951	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code. This issue affects: QNAP Systems Inc. Music Station versions prior to 5.1.13; versions prior to 5.2.9; versions prior to 5.3.11.	6.1	More Details
CVE-2018-19954	The cross-site scripting vulnerability has been reported to affect earlier versions of Photo Station. If exploited, the vulnerability could allow remote attackers to inject malicious code. This issue affects: QNAP Systems Inc. Photo Station versions prior to 5.7.11; versions prior to 6.0.10.	6.1	More Details
CVE-2018-19955	The cross-site scripting vulnerability has been reported to affect earlier versions of Photo Station. If exploited, the vulnerability could allow remote attackers to inject malicious code. This issue affects: QNAP Systems Inc. Photo Station versions prior to 5.7.11; versions prior to 6.0.10.	6.1	More Details
CVE-2018-19956	The cross-site scripting vulnerability has been reported to affect earlier versions of Photo Station. If exploited, the vulnerability could allow remote attackers to inject malicious code. This issue affects: QNAP Systems Inc. Photo Station versions prior to 5.7.11; versions prior to 6.0.10.	6.1	More Details
CVE-2020-27885	Cross-Site Scripting (XSS) vulnerability on WSO2 API Manager 3.1.0. By exploiting a Cross-site scripting vulnerability the attacker can hijack a logged-in user’s session by stealing cookies which means that a malicious hacker can change the logged-in user’s password and invalidate the session of the victim while the hacker maintains access.	6.1	More Details
CVE-2020-24303	Grafana before 7.1.0-beta 1 allows XSS via a query alias for the ElasticSearch datasource.	6.1	More Details
CVE-2020-27741	Multiple cross-site scripting (XSS) vulnerabilities in Citadel WebCit through 926 allow remote attackers to inject arbitrary web script or HTML via multiple pages and parameters. NOTE: this was reported to the vendor in a publicly archived "Multiple Security Vulnerabilities in WebCit 926" thread.	6.1	More Details
CVE-2020-8262	A vulnerability in the Pulse Connect Secure / Pulse Policy Secure below 9.1R9 could allow attackers to conduct Cross-Site Scripting (XSS) and Open Redirection for authenticated user web interface.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27982	IceWarp 11.4.5.0 allows XSS via the language parameter.	6.1	More Details
CVE-2018-19953	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code. QNAP has already fixed the issue in the following QTS versions. QTS 4.4.2.1231 on build 20200302; QTS 4.4.1.1201 on build 20200130; QTS 4.3.6.1218 on build 20200214; QTS 4.3.4.1190 on build 20200107; QTS 4.3.3.1161 on build 20200109; QTS 4.2.6 on build 20200109.	6.1	More Details
CVE-2020-28034	WordPress before 5.5.2 allows XSS associated with global variables.	6.1	More Details
CVE-2020-27974	NeoPost Mail Accounting Software Pro 5.0.6 allows php/Commun/FUS_SCM_BlockStart.php?code= XSS.	6.1	More Details
CVE-2020-5935	On BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM) versions 15.1.0-15.1.0.5, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when handling MQTT traffic through a BIG-IP virtual server associated with an MQTT profile and an iRule performing manipulations on that traffic, TMM may produce a core file.	5.9	More Details
CVE-2020-27650	Synology DiskStation Manager (DSM) before 6.2.3-25426-2 does not set the Secure flag for the session cookie in an HTTPS session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an HTTP session.	5.8	More Details
CVE-2020-27651	Synology Router Manager (SRM) before 1.2.4-8081 does not set the Secure flag for the session cookie in an HTTPS session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an HTTP session.	5.8	More Details
CVE-2020-15989	Uninitialized data in PDFium in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	5.5	More Details
CVE-2020-14323	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.	5.5	More Details
CVE-2020-25204	The God Kings application 0.60.1 for Android exposes a broadcast receiver to other apps called com.innogames.core.frontend.notifications.receivers.LocalNotificationBroadcastReceiver. The purpose of this broadcast receiver is to show an in-game push notification to the player. However, the application does not enforce any authorization schema on the broadcast receiver, allowing any application to send fully customizable in-game push notifications.	5.5	More Details
CVE-2020-4785	IBM App Connect Enterprise Certified Container 1.0.0, 1.0.1, 1.0.2, 1.0.3, and 1.0.4 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 189219.	5.4	More Details
CVE-2020-8263	A vulnerability in the authenticated user web interface of Pulse Connect Secure < 9.1R9 could allow attackers to conduct Cross-Site Scripting (XSS) through the CGI file.	5.4	More Details
CVE-2020-27957	The RandomGameUnit extension for MediaWiki through 1.35 was not properly escaping various title-related data. When certain varieties of games were created within MediaWiki, their names or titles could be manipulated to generate stored XSS within the RandomGameUnit extension.	5.4	More Details
CVE-2020-27980	Genexis Platinum-4410 P4410-V2-1.28 devices allow stored XSS in the WLAN SSID parameter. This could allow an attacker to perform malicious actions in which the XSS popup will affect all privileged users.	5.4	More Details
CVE-2020-24709	Cross Site Scripting (XSS) vulnerability in Gophish through 0.10.1 via a crafted landing page or email template.	5.4	More Details
CVE-2020-24712	Cross Site Scripting (XSS) vulnerability in Gophish before 0.11.0 via the IMAP Host field on the account settings page.	5.4	More Details
CVE-2020-23989	NeDi 1.9C allows pwsec.php oid XSS.	5.4	More Details
CVE-2020-23868	NeDi 1.9C allows inc/rt-popup.php d XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25516	WSO2 Enterprise Integrator 6.6.0 or earlier contains a stored cross-site scripting (XSS) vulnerability in BPMN explorer tasks.	5.4	More Details
CVE-2020-15914	A cross-site scripting (XSS) vulnerability exists in the Origin Client for Mac and PC 10.5.86 or earlier that could allow a remote attacker to execute arbitrary Javascript in a target user's Origin client. An attacker could use this vulnerability to access sensitive data related to the target user's Origin account, or to control or monitor the Origin text chat window.	5.4	More Details
CVE-2020-24708	Cross Site Scripting (XSS) vulnerability in Gophish before 0.11.0 via the Host field on the send profile form.	5.4	More Details
CVE-2020-27359	A cross-site scripting (XSS) issue in REDCap 8.11.6 through 9.x before 10 allows attackers to inject arbitrary JavaScript or HTML in the Messenger feature. It was found that the filename of the image or file attached in a message could be used to perform this XSS attack. A user could craft a message and send it to anyone on the platform including admins. The XSS payload would execute on the other account without interaction from the user on several pages.	5.4	More Details
CVE-2020-28002	In SonarQube 8.4.2.36762, an external attacker can achieve authentication bypass through SonarScanner. With an empty value for the -D sonar.login option, anonymous authentication is forced. This allows creating and overwriting public and private projects via the /api/ce/submit endpoint.	5.3	More Details
CVE-2020-6829	When performing EC scalar point multiplication, the wNAF point multiplication algorithm was used; which leaked partial information about the nonce used during signature generation. Given an electro-magnetic trace of a few signature generations, the private key could have been computed. This vulnerability affects Firefox < 80 and Firefox for Android < 80.	5.3	More Details
CVE-2020-7760	This affects the package codemirror before 5.58.2; the package org.apache.marmotta.webjars:codemirror before 5.58.2. The vulnerable regular expression is located in https://github.com/codemirror/CodeMirror/blob/cdb228ac736369c685865b122b736cd0d397836c/mode/javascript/javascript.jsL129. The ReDOS vulnerability of the regex is mainly due to the sub-pattern (sl/*.*?*/)*	5.3	More Details
CVE-2020-27993	Hrsale 2.0.0 allows download?type=files&filename=../ directory traversal to read arbitrary files.	5.3	More Details
CVE-2019-4563	IBM Security Directory Server 6.4.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 166624.	5.3	More Details
CVE-2019-4547	IBM Security Directory Server 6.4.0 generates an error message that includes sensitive information about its environment, users, or associated data. IBM X-Force ID: 165949.	5.3	More Details
CVE-2020-25689	A memory leak flaw was found in WildFly in all versions up to 21.0.0.Final, where host-controller tries to reconnect in a loop, generating new connections which are not properly closed while not able to connect to domain-controller. This flaw allows an attacker to cause an Out of memory (OOM) issue, leading to a denial of service. The highest threat from this vulnerability is to system availability.	5.3	More Details
CVE-2020-28042	ServiceStack before 5.9.2 mishandles JWT signature verification unless an application has a custom ValidateToken function that establishes a valid minimum length for a signature.	5.3	More Details
CVE-2020-27740	Citadel WebCit through 926 allows unauthenticated remote attackers to enumerate valid users within the platform. NOTE: this was reported to the vendor in a publicly archived "Multiple Security Vulnerabilities in WebCit 926" thread.	5.3	More Details
CVE-2020-26939	In Legion of the Bouncy Castle BC before 1.61 and BC-FJA before 1.0.1.2, attackers can obtain sensitive information about a private exponent because of Observable Differences in Behavior to Error Inputs. This occurs in org.bouncycastle.crypto.encodings.OAEPEncoding. Sending invalid ciphertext that decrypts to a short payload in the OAEP Decoder could result in the throwing of an early exception, potentially leaking some information about the private exponent of the RSA private key performing the encryption.	5.3	More Details
CVE-2020-24710	Gophish before 0.11.0 allows SSRF attacks.	5.3	More Details
CVE-2020-11484	NVIDIA DGX servers, all DGX-1 with BMC firmware versions prior to 3.38.30, contains a vulnerability in the AMI BMC firmware in which an attacker with administrative privileges can obtain the hash of the BMC/IPMI user password, which may lead to information disclosure.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8255	A vulnerability in the Pulse Connect Secure < 9.1R9 admin web interface could allow an authenticated attacker to perform an arbitrary file reading vulnerability is fixed using encrypted URL blacklisting that prevents these messages.	4.9	More Details
CVE-2020-5932	On BIG-IP ASM 15.1.0-15.1.0.5, a cross-site scripting (XSS) vulnerability exists in the BIG-IP ASM Configuration utility response and blocking pages. An authenticated user with administrative privileges can specify a response page with any content, including JavaScript code that will be executed when preview is opened.	4.8	More Details
CVE-2020-1908	Improper authorization of the Screen Lock feature in WhatsApp and WhatsApp Business for iOS prior to v2.20.100 could have permitted use of Siri to interact with the WhatsApp application even after the phone was locked.	4.6	More Details
CVE-2020-27015	Trend Micro Antivirus for Mac 2020 (Consumer) contains an Error Message Information Disclosure vulnerability that if exploited, could allow kernel pointers and debug messages to leak to userland. An attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability.	4.4	More Details
CVE-2020-4649	IBM Planning Analytics Local 2.0.9.2 and IBM Planning Analytics Workspace 57 could expose data to non-privleged users by not invalidating TM1Web user sessions. IBM X-Force ID: 186022.	4.3	More Details
CVE-2020-28031	eramba through c2.8.1 allows HTTP Host header injection with (for example) resultant wkhtml2pdf PDF printing by authenticated users.	4.3	More Details
CVE-2020-27358	An issue was discovered in REDCap 8.11.6 through 9.x before 10. The messenger's CSV feature (that allows users to export their conversation threads as CSV) allows non-privileged users to export one another's conversation threads by changing the thread_id parameter in the request to the endpoint Messenger/messenger_download_csv.php?title=Hey&thread_id={THREAD_ID}.	4.3	More Details
CVE-2020-8261	A vulnerability in the Pulse Connect Secure / Pulse Policy Secure < 9.1R9 is vulnerable to arbitrary cookie injection.	4.3	More Details
CVE-2020-4864	IBM Resilient SOAR V38.0 could allow an attacker on the internal net work to provide the server with a spoofed source IP address. IBM X-Force ID: 190567.	4.3	More Details
CVE-2020-28040	WordPress before 5.5.2 allows CSRF attacks that change a theme's background image.	4.3	More Details
CVE-2020-15703	There is no input validation on the Locale property in an apt transaction. An unprivileged user can supply a full path to a writable directory, which lets aptd read a file as root. Having a symlink in place results in an error message if the file exists, and no error otherwise. This way an unprivileged user can check for the existence of any files on the system as root.	4.0	More Details
CVE-2019-4349	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 applications can be installed on a deprecated operating system version that could compromised the confidentiality and integrity of the service. IBM X-Force ID: 161486	3.5	More Details
CVE-2020-25374	CyberArk Privileged Session Manager (PSM) 10.9.0.15 allows attackers to discover internal pathnames by reading an error popup message after two hours of idle time.	2.6	More Details
CVE-2020-8173	A too small set of random characters being used for encryption in Nextcloud Server 18.0.4 allowed decryption in shorter time than intended.	2.2	More Details
CVE-2020-27981	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