SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 March 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-2020-8598	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow a remote attacker to execute arbitrary code on affected installations with SYSTEM level privileges. Authentication is not required to exploit this vulnerability.	9.8	More Details
CVE-2020-1944	There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and Transfer-Encoding and Content length headers. Upgrade to versions 7.1.9 and 8.0.6 or later versions.	9.8	More Details
CVE-2019-20567	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. A up_parm heap overflow leads to code execution in the bootloader. The Samsung ID is SVE-2019-14993 (September 2019).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20566	An issue was discovered on Samsung mobile devices with any (before September 2019 for SMP1300 Exynos modem chipsets) software. Attackers can trigger stack corruption in the Shannon modem via a crafted RP-Originator/Destination address. The Samsung ID is SVE-2019-14858 (September 2019).	9.8	More Details
CVE-2019-20563	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. The SEC_FR trustlet has an out of bounds write. The Samsung ID is SVE-2019-15272 (October 2019).	9.8	More Details
CVE-2019-20562	An issue was discovered on Samsung mobile devices with P(9.0) (with TEEGRIS) software. There is a buffer overflow in the BIOSUB Trustlet. The Samsung ID is SVE-2019-15264 (October 2019).	9.8	More Details
CVE-2019-20561	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. The bootloader has an integer signedness error. The Samsung ID is SVE-2019-15230 (October 2019).	9.8	More Details
CVE-2019-20560	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. The BIOSUB Trustlet has an out of bounds write. The Samsung ID is SVE-2019-15261 (October 2019).	9.8	More Details
CVE-2019-20558	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. There is a Buffer Overflow in the Touch Screen Driver. The Samsung ID is SVE-2019-14990 (October 2019).	9.8	More Details
CVE-2019-20556	An issue was discovered on Samsung mobile devices with P(9.0) (SM6150, SM8150, SM8150_FUSION, exynos7885, exynos9610, and exynos9820 chipsets) software. RKP memory corruption allows attackers to control the effective address in EL2. The Samsung ID is SVE-2019-15221 (October 2019).	9.8	More Details
CVE-2019-20553	An issue was discovered on Samsung mobile devices with P(9.0) (SM6150, SM8150, SM8150_FUSION, exynos7885, exynos9610, and exynos9820 chipsets) software. Arbitrary memory read and write operations can occur in RKP. The Samsung ID is SVE-2019-15143 (October 2019).	9.8	More Details
CVE-2019-20549	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Broadcom chipsets) software. A heap out-of-bounds access can occur during LE Packet reception in Broadcom Bluetooth. The Samsung ID is SVE-2019-15724 (November 2019).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20548	An issue was discovered on Samsung mobile devices with P(9.0) devices (Qualcomm chipsets) software. There is a buffer overflow in the bootloader. The Samsung ID is SVE-2019-15399 (November 2019).	9.8	More Details
CVE-2020-10850	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. The secure bootloade has a buffer overflow of the USB buffer, leading to arbitrary code execution. The Samsung ID is SVE-2019-15872 (January 2020).	9.8	More Details
CVE-2020-10849	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos7885, Exynos8895, and Exynos9810 chipsets) software. The Gatekeeper trustlet allows a brute-force attack on the screen lock password. The Samsung ID is SVE-2019-14575 (January 2020).	9.8	More Details
CVE-2020-10848	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos 9810 chipsets) software. Arbitrary memory mapping exists in TEE. The Samsung ID is SVE-2019-16665 (February 2020).	9.8	More Details
CVE-2020-10837	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (with TEEGRIS) software. The Esecomm Trustlet allows a stack overflow and arbitrary code execution. The Samsung ID is SVE-2019-15984 (February 2020).	9.8	More Details
CVE-2020-10836	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (Exynos chipsets) software. The Widevine Trustlet allows read and write operations on arbitrary memory locations. The Samsung ID is SVE-2019-15873 (February 2020).	9.8	More Details
CVE-2020-10835	An issue was discovered on Samsung mobile devices with any (before February 2020 for Exynos modem chipsets) software. There is a buffer overflow in baseband CP message decoding. The Samsung IDs are SVE-2019-15816 and SVE-2019-15817 (February 2020).	9.8	More Details
CVE-2019-20545	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos chipsets) software. A buffer overflow in the HDCP Trustlet affects secure TEEGRIS memory. The Samsung ID is SVE-2019-15283 (November 2019).	9.8	More Details
CVE-2019-20544	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos chipsets) software. There is an out-of-bounds write in the ICCC Trustlet. The Samsung ID is SVE-2019-15274 (November 2019).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20537	An issue was discovered on Samsung mobile devices with P(9.0) (TEEGRIS and Qualcomm chipsets). There is arbitrary memory overwrite in the SEM Trustlet, leading to arbitrary code execution. The Samsung IDs are SVE-2019-14651, SVE-2019-14666 (November 2019).	9.8	More Details
CVE-2019-20536	An issue was discovered on Samsung mobile devices with N(7.1), O(8.x), and P(9.0) (released in China) software. The Firewall application mishandles the PermissionWhiteLists protection mechanism. The Samsung ID is SVE-2019-14299 (November 2019).	9.8	More Details
CVE-2019-20530	An issue was discovered on Samsung mobile devices with N(7.1), O(8.x), P(9.0), and Q(10.0) software. Arbitrary code execution is possible on the lock screen. The Samsung ID is SVE-2019-15266 (December 2019).	9.8	More Details
CVE-2020-10938	GraphicsMagick before 1.3.35 has an integer overflow and resultant heap-based buffer overflow in HuffmanDecodeImage in magick/compress.c.	9.8	More Details
CVE-2019-20571	An issue was discovered on Samsung mobile devices with O(8.x) (with TEEGRIS) software. There is type confusion in the WVDRM Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14885 (September 2019).	9.8	More Details
CVE-2019-20572	An issue was discovered on Samsung mobile devices with O(8.1) and P(9.0) (Exynos chipsets) software. load_kernel has a buffer overflow via untrusted data. The Samsung ID is SVE-2019-14939 (September 2019).	9.8	More Details
CVE-2019-20578	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos 9820 chipsets) software. A Buffer overflow occurs when loading the UH Partition during Secure Boot. The Samsung ID is SVE-2019-14412 (August 2019).	9.8	More Details
CVE-2019-20605	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. A heap overflow occurs for baseband in the Shannon modem. The Samsung ID is SVE-2019-14071 (May 2019).	9.8	More Details
CVE-2020-7007	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the attacker may execute arbitrary codes or target the device, causing it to go out of service.	9.8	More Details
CVE-2020-6991	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, weak password requirements may allow an attacker to gain access using brute force.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6981	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, an attacker may gain access to the system without proper authentication.	9.8	More Details
CVE-2020-6072	An exploitable code execution vulnerability exists in the label-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing compressed labels in mDNS messages, the rr_decode function's return value is not checked, leading to a double free that could be exploited to execute arbitrary code. An attacker can send an mDNS message to trigger this vulnerability.	9.8	More Details
CVE-2020-6995	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the application utilizes weak password requirements, which may allow an attacker to gain unauthorized access.	9.8	More Details
CVE-2020-6985	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, these devices use a hard-coded service code for access to the console.	9.8	More Details
CVE-2019-20622	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. There is a baseband stack overflow. The Samsung ID is SVE-2018-13188 (February 2019).	9.8	More Details
CVE-2019-20621	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. There is a baseband heap overflow. The Samsung ID is SVE-2018-13187 (February 2019).	9.8	More Details
CVE-2019-20611	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), Go(8.1), P(9.0), and Go(9.0) (Exynos chipsets) software. A baseband stack overflow leads to arbitrary code execution. The Samsung ID is SVE-2019-13963 (April 2019).	9.8	More Details
CVE-2019-20607	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (MSM8996, MSM8998, Exynos7420, Exynos7870, Exynos8890, and Exynos8895 chipsets) software. A heap overflow in the keymaster Trustlet allows attackers to write to TEE memory, and achieve arbitrary code execution. The Samsung ID is SVE-2019-14126 (May 2019).	9.8	More Details
CVE-2019-20590	An issue was discovered on Samsung mobile devices with O(8.x) (Qualcomm chipsets) software. There is an integer underflow in the Secure Storage Trustlet. The Samsung ID is SVE-2019-13952 (July 2019).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20581	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. A stack overflow in the HDCP Trustlet causes arbitrary code execution. The Samsung ID is SVE-2019-14665 (August 2019).	9.8	More Details
CVE-2019-20576	An issue was discovered on Samsung mobile devices with P(9.0) software. The MemorySaver Content Provider allows SQL injection. The Samsung ID is SVE-2019-14365 (August 2019).	9.8	More Details
CVE-2020-6989	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, a buffer overflow in the web server allows remote attackers to cause a denial-of-service condition or execute arbitrary code.	9.8	More Details
CVE-2019-20589	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the SKPM Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14892 (August 2019).	9.8	More Details
CVE-2019-20588	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the SEM Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14891 (August 2019).	9.8	More Details
CVE-2019-20587	An issue was discovered on Samsung mobile devices with O(8.1) and P(9.0) (with TEEGRIS) software. There is type confusion in the MLDAP Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14867 (August 2019).	9.8	More Details
CVE-2019-20586	An issue was discovered on Samsung mobile devices with O(8.1) and P(9.0) (with TEEGRIS) software. There is type confusion in the FINGERPRINT Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14864 (August 2019).	9.8	More Details
CVE-2019-20585	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the SEC_FR Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14851 (August 2019).	9.8	More Details
CVE-2019-20584	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the HDCP Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14850 (August 2019).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20583	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (with TEEGRIS) software. There is type confusion in the EXT_FR Trustlet, leading to arbitrary code execution. The Samsung ID is SVE-2019-14847 (August 2019).	9.8	More Details
CVE-2019-20582	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) devices (Exynos9810 chipsets) software. There is a use after free in the ion driver. The Samsung ID is SVE-2019-14837 (August 2019).	9.8	More Details
CVE-2020-8599	Trend Micro Apex One (2019) and OfficeScan XG server contain a vulnerable EXE file that could allow a remote attacker to write arbitrary data to an arbitrary path on affected installations and bypass ROOT login. Authentication is not required to exploit this vulnerability.	9.8	More Details
CVE-2020-1747	A vulnerability was discovered in the PyYAML library in versions before 5.3.1, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. An attacker could use this flaw to execute arbitrary code on the system by abusing the python/object/new constructor.	9.8	More Details
CVE-2020-10879	rConfig before 3.9.5 allows command injection by sending a crafted GET request to lib/crud/search.crud.php since the nodeId parameter is passed directly to the exec function without being escaped.	9.8	More Details
CVE-2020-10674	PerlSpeak through 2.01 allows attackers to execute arbitrary OS commands, as demonstrated by use of system and 2-argument open.	9.8	More Details
CVE-2019-16072	An OS command injection vulnerability in the discover_and_manage CGI script in NETSAS Enigma NMS 65.0.0 and prior allows an attacker to execute arbitrary code because of improper neutralization of shell metacharacters in the ip_address variable within an snmp_browser action.	9.8	More Details
CVE-2019-17565	There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and chunked encoding. Upgrade to versions 7.1.9 and 8.0.6 or later versions.	9.8	More Details
CVE-2019-12127	In ONAP OOM through Dublin, by accessing an applicable port (30234, 30290, 32010, 30270, 30224, 30281, 30254, 30285, and/or 30271), an attacker gains full access to the respective ONAP services without any authentication. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12126	In ONAP DCAE through Dublin, by accessing an applicable port (30234, 30290, 32010, 30270, 30224, 30281, 30254, 30285, and/or 30271), an attacker gains full access to the respective ONAP services without any authentication. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12125	In ONAP Logging through Dublin, by accessing an applicable port (30234, 30290, 32010, 30270, 30224, 30281, 30254, 30285, and/or 30271), an attacker gains full access to the respective ONAP services without any authentication. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-16382	An issue was discovered in Ivanti Workspace Control 10.3.110.0. One is able to bypass Ivanti's FileGuard folder protection by renaming the WMTemp work folder used by PowerGrid. A malicious PowerGrid XML file can then be created, after which the folder is renamed back to its original value. Also, CVE-2018-15591 exploitation can consequently be achieved by using PowerGrid with the /SEE parameter to execute the arbitrary command specified in the XML file.	9.8	More Details
CVE-2019-12130	In ONAP CLI through Dublin, by accessing an applicable port (30234, 30290, 32010, 30270, 30224, 30281, 30254, 30285, and/or 30271), an attacker gains full access to the respective ONAP services without any authentication. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12129	In ONAP MSB through Dublin, by accessing an applicable port (30234, 30290, 32010, 30270, 30224, 30281, 30254, 30285, and/or 30271), an attacker gains full access to the respective ONAP services without any authentication. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12128	In ONAP SO through Dublin, by accessing an applicable port (30234, 30290, 32010, 30270, 30224, 30281, 30254, 30285, and/or 30271), an attacker gains full access to the respective ONAP services without any authentication. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2020-9423	LogicalDoc before 8.3.3 could allow an attacker to upload arbitrary files, leading to command execution or retrieval of data from the database. LogicalDoc provides a functionality to add documents. Those documents could then be used for multiple tasks, such as version control, shared among users, applying tags, etc. This functionality could be abused by an unauthenticated attacker to upload an arbitrary file in a restricted folder. This would lead to the executions of malicious commands with root privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12132	An issue was discovered in ONAP SDNC before Dublin. By executing sla/dgUpload with a crafted filename parameter, an unauthenticated attacker can execute an arbitrary command. All SDC setups that include admportal are affected.	9.8	More Details
CVE-2019-19148	Tellabs Optical Line Terminal (OLT) 1150 devices allow Remote Command Execution via the -l option to TELNET or SSH. Tellabs has addressed this issue in the SR30.1 and SR31.1 release on February 18, 2020.	9.8	More Details
CVE-2019-12120	An issue was discovered in ONAP VNFSDK through Dublin. By accessing port 8000 of demo-vnfsdk-vnfsdk, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12119	An issue was discovered in ONAP SDC through Dublin. By accessing port 7000 of demo-sdc-sdc-wfd-fe pod, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12118	An issue was discovered in ONAP SDC through Dublin. By accessing port 7001 of demo-sdc-sdc-wfd-be pod, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12117	An issue was discovered in ONAP SDC through Dublin. By accessing port 4001 of demo-sdc-sdc-onboarding-be pod, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12116	An issue was discovered in ONAP SDC through Dublin. By accessing port 6000 of demo-sdc-sdc-fe pod, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12115	An issue was discovered in ONAP SDC through Dublin. By accessing port 4000 of demo-sdc-sdc-be pod, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12114	An issue was discovered in ONAP HOLMES before Dublin. By accessing port 9202 of dep-holmes-engine-mgmt pod, an unauthenticated attacker (who already has access to pod-to-pod communication) may execute arbitrary code inside that pod. All ONAP Operations Manager (OOM) setups are affected.	9.8	More Details
CVE-2019-12112	An issue was discovered in ONAP SDNC before Dublin. By executing sla/upload with a crafted filename parameter, an unauthenticated attacker can execute an arbitrary command. All SDC setups that include admportal are affected.	9.8	More Details
CVE-2020-3922	LisoMail, by ArmorX, allows SQL Injections, attackers can access the database without authentication via a URL parameter manipulation.	9.8	More Details
CVE-2020-8600	Trend Micro Worry-Free Business Security (9.0, 9.5, 10.0) is affected by a directory traversal vulnerability that could allow an attacker to manipulate a key file to bypass authentication.	9.8	More Details
CVE-2018-20334	An issue was discovered in ASUSWRT 3.0.0.4.384.20308. When processing the /start_apply.htm POST data, there is a command injection issue via shell metacharacters in the fb_email parameter. By using this issue, an attacker can control the router and get shell.	9.8	More Details
CVE-2020-8986	lib/NSSDropbox.php in ZendTo prior to 5.22-2 Beta failed to properly check for equality when validating the session cookie, allowing an attacker to gain administrative access with a large number of requests.	9.8	More Details
CVE-2019-12498	The WP Live Chat Support plugin before 8.0.33 for WordPress accepts certain REST API calls without invoking the wplc_api_permission_check protection mechanism.	9.8	More Details
CVE-2019-20627	AutoUpdater.cs in AutoUpdater.NET before 1.5.8 allows XXE.	9.8	More Details
CVE-2020-7475	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), reflective DLL, vulnerability exists in EcoStruxure Control Expert (all versions prior to 14.1 Hot Fix), Unity Pro (all versions), Modicon M340 (all versions prior to V3.20), Modicon M580 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5722	The HTTP interface of the Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via crafted HTTP request. An attacker can use this vulnerability to execute shell commands as root on versions before 1.0.19.20 or inject HTML in password recovery emails in versions before 1.0.20.17.	9.8	More Details
CVE-2020-7480	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists in Andover Continuum (All versions), which could cause files on the application server filesystem to be viewable when an attacker interferes with an application's processing of XML data.	9.8	More Details
CVE-2020-7961	Deserialization of Untrusted Data in Liferay Portal prior to 7.2.1 CE GA2 allows remote attackers to execute arbitrary code via JSON web services (JSONWS).	9.8	More Details
CVE-2020-6967	In Rockwell Automation all versions of FactoryTalk Diagnostics software, a subsystem of the FactoryTalk Services Platform, FactoryTalk Diagnostics exposes a .NET Remoting endpoint via RNADiagnosticsSrv.exe at TCPtcp/8082, which can insecurely deserialize untrusted data.	9.8	More Details
CVE-2020-8868	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight Evolve 9.0.0. Authentication is not required to exploit this vulnerability. The specific flaw exists within the __service__ user account. The product contains a hard-coded password for this account. An attacker can leverage this vulnerability to execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-9553.	9.8	More Details
CVE-2019-17559	There is a vulnerability in Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.8, and 8.0.0 to 8.0.5 with a smuggling attack and scheme parsing. Upgrade to versions 7.1.9 and 8.0.6 or later versions.	9.8	More Details
CVE-2020-9752	Naver Cloud Explorer before 2.2.2.11 allows the attacker can move a local file in any path on the filesystem as a system privilege through its named pipe.	9.8	More Details
CVE-2020-10806	eZ Publish Kernel before 5.4.14.1, 6.x before 6.13.6.2, and 7.x before 7.5.6.2 and eZ Publish Legacy before 5.4.14.1, 2017 before 2017.12.7.2, and 2019 before 2019.03.4.2 allow remote attackers to execute arbitrary code by uploading PHP code, unless the vhost configuration permits only app.php execution.	9.8	More Details
CVE-2019-12767	An issue was discovered on D-Link DAP-1650 devices before 1.04B02_J65H Hot Fix. Attackers can execute arbitrary commands.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-7487	On Swann DVR04B, DVR08B, DVR-16CIF, and DVR16B devices, raysharpdvr application has a vulnerable call to “system”, which allows remote attackers to execute arbitrary code via TCP port 9000.	9.8	More Details
CVE-2020-10799	The svglib package through 0.9.3 for Python allows XXE attacks via an svg2rlg call.	9.8	More Details
CVE-2019-11574	An issue was discovered in Simple Machines Forum (SMF) before release 2.0.17. There is SSRF related to Subs-Package.php and Subs.php because user-supplied data is used directly in curl calls.	9.8	More Details
CVE-2019-18641	Rock RMS before 1.8.6 mishandles vCard access control within the People/GetVCard/REST controller.	9.8	More Details
CVE-2019-15522	An issue was discovered in LINBIT csync2 through 2.0. csync_daemon_session in daemon.c neglects to force a failure of a hello command when the configuration requires use of SSL.	9.8	More Details
CVE-2020-8137	Code injection vulnerability in blamer 1.0.0 and earlier may result in remote code execution when the input can be controlled by an attacker.	9.8	More Details
CVE-2020-8135	The uppy npm package < 1.9.3 is vulnerable to a Server-Side Request Forgery (SSRF) vulnerability, which allows an attacker to scan local or external network or otherwise interact with internal systems.	9.8	More Details
CVE-2020-9760	An issue was discovered in WeeChat before 2.7.1 (0.3.4 to 2.7 are affected). When a new IRC message 005 is received with longer nick prefixes, a buffer overflow and possibly a crash can happen when a new mode is set for a nick.	9.8	More Details
CVE-2019-16064	NETSAS Enigma NMS 65.0.0 and prior suffers from a directory traversal vulnerability that can allow an authenticated user to access files and directories stored outside of the web root folder. By exploiting this vulnerability, it is possible for an attacker to list operating-system directory contents on the server, create directories and upload files in permissible locations, and modify filenames and delete files that are accessible by the user running the web server instance.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19676	A CSV injection in arxes-tolina 3.0.0 allows malicious users to gain remote control of other computers. By entering formula code in the following columns: Kundennummer, Firma, Street, PLZ, Ort, Zahlziel, and Bemerkung, an attacker can create a user with a name that contains malicious code. Other users might download this data as a CSV file and corrupt their PC by opening it in a tool such as Microsoft Excel. The attacker could gain remote access to the user's PC.	9.6	More Details
CVE-2019-20606	An issue was discovered on Samsung mobile devices with any (before May 2019) software. A phishing attack against OMACP can change the network and internet settings. The Samsung ID is SVE-2019-14073 (May 2019).	9.3	More Details
CVE-2019-6560	In Auto-Maskin RP210E Versions 3.7 and prior, DCU210E Versions 3.7 and prior and Marine Observer Pro (Android App), the software contains a mechanism for users to recover or change their passwords without knowing the original password, but the mechanism is weak.	9.1	More Details
CVE-2019-12124	An issue was discovered in ONAP APPC before Dublin. By using an exposed unprotected Jolokia interface, an unauthenticated attacker can read or overwrite an arbitrary file. All APPC setups are affected.	9.1	More Details
CVE-2019-20597	An issue was discovered on Samsung mobile devices with N(7.1), O(8.x), and P(9.0) software. SPENgesture allows arbitrary applications to read or modify user-input logs. The Samsung ID is SVE-2019-14170 (June 2019).	9.1	More Details
CVE-2019-12131	An issue was detected in ONAP APPC through Dublin and SDC through Dublin. By setting a USER_ID parameter in an HTTP header, an attacker may impersonate an arbitrary existing user without any authentication. All APPC and SDC setups are affected.	9.1	More Details
CVE-2020-10661	HashiCorp Vault and Vault Enterprise versions 0.11.0 through 1.3.3 may, under certain circumstances, have existing nested-path policies grant access to Namespaces created after-the-fact. Fixed in 1.3.4.	9.1	More Details
CVE-2020-6972	In Notifier Web Server (NWS) Version 3.50 and earlier, the Honeywell Fire Web Server’s authentication may be bypassed by a capture-replay attack from a web browser.	9.1	More Details
CVE-2019-20596	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) (Exynos chipsets) software. There is information disclosure in the GateKeeper Trustlet. The Samsung ID is SVE-2019-13958 (June 2019).	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2014-2721	In FortiBalancer 400, 1000, 2000 and 3000, a platform-specific remote access vulnerability has been discovered that may allow a remote user to gain privileged access to affected systems using SSH. The vulnerability is caused by a configuration error, and is not the result of an underlying SSH defect.	8.8	More Details
CVE-2020-10672	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.aries.transaction.jms.internal.XaPooledConnectionFactory (aka aries.transaction.jms).	8.8	More Details
CVE-2020-6424	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6427	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2019-12113	An issue was discovered in ONAP SDNC before Dublin. By executing sla/printAsGv with a crafted module parameter, an authenticated user can execute an arbitrary command. All SDC setups that include admportal are affected.	8.8	More Details
CVE-2020-6428	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6429	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2019-12123	An issue was discovered in ONAP SDNC before Dublin. By executing sla/printAsXml with a crafted module parameter, an authenticated user can execute an arbitrary command. All SDC setups that include admportal are affected.	8.8	More Details
CVE-2020-6449	Use after free in audio in Google Chrome prior to 80.0.3987.149 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-2020-8875	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the IOCTL handler. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-10028.	8.8	More Details
CVE-2019-16066	An unrestricted file upload vulnerability exists in user and system file upload functions in NETSAS Enigma NMS 65.0.0 and prior. This allows an attacker to upload malicious files and perform arbitrary code execution on the system.	8.8	More Details
CVE-2019-16065	A remote SQL injection web vulnerability was discovered in the Enigma NMS 65.0.0 and prior web application that allows an attacker to execute SQL commands to expose and compromise the web server, expose database tables and values, and potentially execute system-based commands as the mysql user. This affects the search_pattern value of the manage_hosts_short.cgi script.	8.8	More Details
CVE-2019-16061	A number of files on the NETSAS Enigma NMS server 65.0.0 and prior are granted weak world-readable and world-writable permissions, allowing any low privileged user with access to the system to read sensitive data (e.g., .htpasswd) and create/modify/delete content (e.g., under /var/www/html/docs) within the operating system.	8.8	More Details
CVE-2019-11361	Zoho ManageEngine Remote Access Plus 10.0.258 does not validate user permissions properly, allowing for privilege escalation and eventually a full application takeover.	8.8	More Details
CVE-2019-12769	SolarWinds Serv-U Managed File Transfer (MFT) Web client before 15.1.6 Hotfix 2 is vulnerable to Cross-Site Request Forgery in the file upload functionality via ?Command=Upload with the Dir and File parameters.	8.8	More Details
CVE-2020-8863	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper implementation of the authentication algorithm. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-9470.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8864	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.10B04. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of empty passwords. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9471.	8.8	More Details
CVE-2020-4253	IBM Content Navigator 3.0CD does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 175559.	8.8	More Details
CVE-2014-2723	In FortiBalancer 400, 1000, 2000 and 3000, a platform-specific remote access vulnerability has been discovered that may allow a remote user to gain privileged access to affected systems using SSH. The vulnerability is caused by a configuration error, and is not the result of an underlying SSH defect.	8.8	More Details
CVE-2014-2722	In FortiBalancer 400, 1000, 2000 and 3000, a platform-specific remote access vulnerability has been discovered that may allow a remote user to gain privileged access to affected systems using SSH. The vulnerability is caused by a configuration error, and is not the result of an underlying SSH defect.	8.8	More Details
CVE-2020-10678	In Octopus Deploy before 2020.1.5, for customers running on-premises Active Directory linked to their Octopus server, an authenticated user can leverage a bug to escalate privileges.	8.8	More Details
CVE-2020-6422	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2020-6420	Insufficient policy enforcement in media in Google Chrome prior to 80.0.3987.132 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10793	CodeIgniter through 4.0.0 allows remote attackers to gain privileges via a modified Email ID to the "Select Role of the User" page. NOTE: A contributor to the CodeIgniter framework argues that the issue should not be attributed to CodeIgniter. Furthermore, the blog post reference shows an unknown website built with the CodeIgniter framework but that CodeIgniter is not responsible for introducing this issue because the framework has never provided a login screen, nor any kind of login or user management facilities beyond a Session library. Also, another reporter indicates the issue is with a custom module/plugin to CodeIgniter, not CodeIgniter itself.	8.8	More Details
CVE-2020-8881	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of TIF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9774.	8.8	More Details
CVE-2020-8467	A migration tool component of Trend Micro Apex One (2019) and OfficeScan XG contains a vulnerability which could allow remote attackers to execute arbitrary code on affected installations (RCE). An attempted attack requires user authentication.	8.8	More Details
CVE-2020-8468	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication.	8.8	More Details
CVE-2019-19487	Command Injection in minPlayCommand.php in Centreon (19.04.4 and below) allows an attacker to achieve command injection via a plugin test.	8.8	More Details
CVE-2020-8985	ZendTo prior to 5.22-2 Beta allowed reflected XSS and CSRF via the unlock.tpl unlock user functionality.	8.8	More Details
CVE-2019-19025	Cloud Native Computing Foundation Harbor prior to 1.8.6 and 1.9.3 allows CSRF in the VMware Harbor Container Registry for the Pivotal Platform.	8.8	More Details
CVE-2019-19023	Cloud Native Computing Foundation Harbor prior to 1.8.6 and 1.9.3 has a Privilege Escalation Vulnerability in the VMware Harbor Container Registry for the Pivotal Platform.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6982	In Honeywell WIN-PAK 4.7.2, Web and prior versions, the header injection vulnerability has been identified, which may allow remote code execution.	8.8	More Details
CVE-2020-8878	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9625.	8.8	More Details
CVE-2020-8880	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9773.	8.8	More Details
CVE-2019-16071	Enigma NMS 65.0.0 and prior allows administrative users to create low-privileged accounts that do not have the ability to modify any settings in the system, only view the components. However, it is possible for a low-privileged user to perform all actions as an administrator by bypassing authorization controls and sending requests to the server in the context of an administrator.	8.8	More Details
CVE-2020-8882	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the PSD files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9811.	8.8	More Details
CVE-2019-16068	A CSRF vulnerability exists in NETSAS ENIGMA NMS version 65.0.0 and prior that could allow an attacker to be able to trick a victim into submitting a malicious manage_files.cgi request. This can be triggered via XSS or an IFRAME tag included within the site.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10671	The Canon Oce Colorwave 500 4.0.0.0 printer's web application is missing any form of CSRF protections. This is a system-wide issue. An attacker could perform administrative actions by targeting a logged-in administrative user. NOTE: this is fixed in the latest version.	8.8	More Details
CVE-2020-7005	In Honeywell WIN-PAK 4.7.2, Web and prior versions, the affected product is vulnerable to a cross-site request forgery, which may allow an attacker to remotely execute arbitrary code.	8.8	More Details
CVE-2020-10808	Vesta Control Panel (VestaCP) through 0.9.8-26 allows Command Injection via the schedule/backup Backup Listing Endpoint. The attacker must be able to create a crafted filename on the server, as demonstrated by an FTP session that renames .bash_logout to a .bash_logout' substring followed by shell metacharacters.	8.8	More Details
CVE-2020-10673	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.caucho.config.types.ResourceRef (aka caucho-quercus).	8.8	More Details
CVE-2020-7006	Systech Corporation NDS-5000 Terminal Server, NDS/5008 (8 Port, RJ45), firmware Version 02D.30. Successful exploitation of this vulnerability could allow information disclosure, limit system availability, and may allow remote code execution.	8.4	More Details
CVE-2020-6650	UPS companion software v1.05 & Prior is affected by ‘Eval Injection’ vulnerability. The software does not neutralize or incorrectly neutralizes code syntax before using the input in a dynamic evaluation call e.g.”eval” in “Update Manager” class when software attempts to see if there are updates available. This results in arbitrary code execution on the machine where software is installed.	8.3	More Details
CVE-2020-8134	Server-side request forgery (SSRF) vulnerability in Ghost CMS < 3.10.0 allows an attacker to scan local or external network or otherwise interact with internal systems.	8.1	More Details
CVE-2019-16012	A vulnerability in the web UI of Cisco SD-WAN Solution vManage software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web UI improperly validates SQL values. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on, or return values from, the underlying database as well as the operating system.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10800	lix through 15.8.7 allows man-in-the-middle attackers to execute arbitrary code by modifying the HTTP client-server data stream so that the Location header is associated with attacker-controlled executable content in the postDownload field.	8.1	More Details
CVE-2020-1864	Some Huawei products have a security vulnerability due to improper authentication. A remote attacker needs to obtain some information and forge the peer device to send specific packets to the affected device. Due to the improper implementation of the authentication function, attackers can exploit the vulnerability to connect to affected devices and execute a series of commands.Affected product versions include:Secospace AntiDDoS8000 versions V500R001C00,V500R001C20,V500R001C60,V500R005C00.	8.1	More Details
CVE-2019-20568	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) devices (Exynos and Qualcomm chipsets) software. A race condition causes a Use-After-Free. The Samsung ID is SVE-2019-15067 (September 2019).	8.1	More Details
CVE-2019-11689	An issue was discovered in ASUSTOR exFAT Driver through 1.0.0.r20. When conducting license validation, exfat.cgi and exfatctl fail to properly validate server responses and pass unsanitized text to the system shell, resulting in code execution as root.	8.1	More Details
CVE-2019-20613	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. There is time-based SQL injection in Contacts. The Samsung ID is SVE-2018-13452 (March 2019).	8.1	More Details
CVE-2019-20610	An issue was discovered on Samsung mobile devices with N(7.X) and O(8.X) (Exynos 7570, 7870, 7880, 7885, 8890, 8895, and 9810 chipsets) software. A double-fetch vulnerability in Trustlet allows arbitrary TEE code execution. The Samsung ID is SVE-2019-13910 (April 2019).	8.1	More Details
CVE-2020-10802	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability has been discovered where certain parameters are not properly escaped when generating certain queries for search actions in libraries/classes/Controllers/Table/TableSearchController.php. An attacker can generate a crafted database or table name. The attack can be performed if a user attempts certain search operations on the malicious database or table.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10804	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was found in retrieval of the current username (in libraries/classes/Server/Privileges.php and libraries/classes/UserPassword.php). A malicious user with access to the server could create a crafted username, and then trick the victim into performing specific actions with that user account (such as editing its privileges).	8.0	More Details
CVE-2020-10684	A flaw was found in Ansible Engine, all versions 2.7.x, 2.8.x and 2.9.x prior to 2.7.17, 2.8.9 and 2.9.6 respectively, when using ansible_facts as a subkey of itself and promoting it to a variable when inject is enabled, overwriting the ansible_facts after the clean. An attacker could take advantage of this by altering the ansible_facts, such as ansible_hosts, users and any other key data which would lead into privilege escalation or code injection.	7.9	More Details
CVE-2020-7479	A CWE-306: Missing Authentication for Critical Function vulnerability exists in IGSS (Versions 14 and prior using the service: IGSSupdate), which could allow a local user to execute processes that otherwise require escalation privileges when sending local network commands to the IGSS Update Service.	7.8	More Details
CVE-2019-20538	An issue was discovered on Samsung mobile devices with P(9.0) software. There is a heap overflow in the knox_kap driver. The Samsung ID is SVE-2019-14857 (November 2019).	7.8	More Details
CVE-2019-20591	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. There is local SQL injection in the Gear VR Service Content Provider. The Samsung ID is SVE-2019-14058 (July 2019).	7.8	More Details
CVE-2020-3265	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain root-level privileges.	7.8	More Details
CVE-2020-3266	A vulnerability in the CLI of Cisco SD-WAN Solution software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20592	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. There is local SQL injection in the Story Video Editor Content Provider. The Samsung ID is SVE-2019-14062 (July 2019).	7.8	More Details
CVE-2019-16338	The tfo_common component in HwordApp.dll in Hancom Office 9.6.1.7634 allows a use-after-free via a crafted .docx file.	7.8	More Details
CVE-2020-7476	A CWE-426: Untrusted Search Path vulnerability exists in ZigBee Installation Kit (Versions prior to 1.0.1), which could cause execution of malicious code when a malicious file is put in the search path.	7.8	More Details
CVE-2019-16337	The hncbd90 component in Hancom Office 9.6.1.9403 allows a use-after-free via an unknown object in a crafted .docx file.	7.8	More Details
CVE-2019-20573	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. There is local SQL injection in the RCS Content Provider. The Samsung IDs are SVE-2019-14059, SVE-2019-14685 (August 2019).	7.8	More Details
CVE-2020-7474	A CWE-427: Uncontrolled Search Path Element vulnerability exists in ProSoft Configurator (v1.002 and prior), for the PMEPXM0100 (H) module, which could cause the execution of untrusted code when using double click to open a project file which may trigger execution of a malicious DLL.	7.8	More Details
CVE-2019-5184	An exploitable double free vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200. A specially crafted XML cache file written to a specific location on the device can cause a heap pointer to be freed twice, resulting in a denial of service and potentially code execution. An attacker can send a specially crafted packet to trigger the parsing of this cache file.	7.8	More Details
CVE-2020-7002	Delta Industrial Automation CNCSoft ScreenEditor, v1.00.96 and prior. Multiple stack-based buffer overflows can be exploited when a valid user opens a specially crafted, malicious input file.	7.8	More Details
CVE-2019-4001	Improper input validation in Druva inSync Client 6.5.0 allows a local, authenticated attacker to execute arbitrary NodeJS code.	7.8	More Details
CVE-2019-20574	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. There is local SQL injection in the Wi-Fi history Content Provider. The Samsung ID is SVE-2019-14061 (August 2019).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18979	Adaware antivirus 12.6.1005.11662 and 12.7.1055.0 has a quarantine flaw that allows privilege escalation. Exploitation uses an NTFS directory junction to restore a malicious DLL from quarantine into the system32 folder.	7.8	More Details
CVE-2020-10682	The Filemanager in CMS Made Simple 2.2.13 allows remote code execution via a .php.jpegd JPEG file, as demonstrated by m1_files[] to admin/moduleinterface.php. The file should be sent as application/octet-stream and contain PHP code (it need not be a valid JPEG file).	7.8	More Details
CVE-2019-20542	An issue was discovered on Samsung mobile devices with N(7.1), O(8.x), and P(9.0) (Exynos chipsets) software. There is a stack overflow in the kernel driver. The Samsung ID is SVE-2019-15034 (November 2019).	7.8	More Details
CVE-2020-10851	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. There is a stack overflow in the kperfmon driver. The Samsung ID is SVE-2019-15876 (January 2020).	7.8	More Details
CVE-2020-10842	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (S.LSI chipsets) software. There is a heap out-of-bounds write in the tsmux driver. The Samsung ID is SVE-2019-16295 (February 2020).	7.8	More Details
CVE-2020-10841	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 9610 chipsets) software. There is an arbitrary kfree in the vipx and vertex drivers. The Samsung ID is SVE-2019-16294 (February 2020).	7.8	More Details
CVE-2020-10838	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. PROCA allows a use-after-free and arbitrary code execution. The Samsung ID is SVE-2019-16132 (February 2020).	7.8	More Details
CVE-2020-10648	Das U-Boot through 2020.01 allows attackers to bypass verified boot restrictions and subsequently boot arbitrary images by providing a crafted FIT image to a system configured to boot the default configuration.	7.8	More Details
CVE-2020-10832	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos chipsets) software. Kernel Wi-Fi drivers allow out-of-bounds Read or Write operations (e.g., a buffer overflow). The Samsung IDs are SVE-2019-16125, SVE-2019-16134, SVE-2019-16158, SVE-2019-16159, SVE-2019-16319, SVE-2019-16320, SVE-2019-16337, SVE-2019-16464, SVE-2019-16465, SVE-2019-16467 (March 2020).	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10829	An issue was discovered on Samsung mobile devices with O(8.0), P(9.0), and Q(10.0) (Broadcom chipsets) software. A kernel driver heap overflow leads to arbitrary code execution. The Samsung ID is SVE-2019-15880 (March 2020).	7.8	More Details
CVE-2020-10852	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. There is a stack overflow in display driver. The Samsung ID is SVE-2019-15877 (January 2020).	7.8	More Details
CVE-2019-20541	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos chipsets) software. The Wi-Fi kernel drivers have a stack overflow. The Samsung IDs are SVE-2019-14965, SVE-2019-14966, SVE-2019-14968, SVE-2019-14969, SVE-2019-14970, SVE-2019-14980, SVE-2019-14981, SVE-2019-14982, SVE-2019-14983, SVE-2019-14984, SVE-2019-15122, SVE-2019-15123 (November 2019).	7.8	More Details
CVE-2020-5262	In EasyBuild before version 4.1.2, the GitHub Personal Access Token (PAT) used by EasyBuild for the GitHub integration features (like `--new-pr`, `--fro,-pr`, etc.) is shown in plain text in EasyBuild debug log files. This issue is fixed in EasyBuild v4.1.2, and in the `master`+ `develop` branches of the `easybuild-framework` repository.	7.7	More Details
CVE-2020-6987	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed.	7.5	More Details
CVE-2020-6080	An exploitable denial-of-service vulnerability exists in the resource allocation handling of Videolabs libmicrodns 0.1.0. When encountering errors while parsing mDNS messages, some allocated data is not freed, possibly leading to a denial-of-service condition via resource exhaustion. An attacker can send one mDNS message repeatedly to trigger this vulnerability through the function rr_read_RR [5] reads the current resource record, except for the RDATA section. This is read by the loop at in rr_read. For each RR type, a different function is called. When the RR type is 0x10, the function rr_read_TXT is called at [6].	7.5	More Details
CVE-2020-7003	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, sensitive information is transmitted over some web applications in clear text.	7.5	More Details
CVE-2019-20565	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) software. Attackers can change the USB configuration without authentication. The Samsung ID is SVE-2018-13300 (September 2019).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6993	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, an attacker can gain access to sensitive information from the web service without authorization.	7.5	More Details
CVE-2020-6071	An exploitable denial-of-service vulnerability exists in the resource record-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing compressed labels in mDNS messages, the compression pointer is followed without checking for recursion, leading to a denial of service. An attacker can send an mDNS message to trigger this vulnerability.	7.5	More Details
CVE-2020-6073	An exploitable denial-of-service vulnerability exists in the TXT record-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing the RDATA section in a TXT record in mDNS messages, multiple integer overflows can be triggered, leading to a denial of service. An attacker can send an mDNS message to trigger this vulnerability.	7.5	More Details
CVE-2019-18936	UniValue::read() in UniValue before 1.0.5 allow attackers to cause a denial of service (the class internal data reaches an inconsistent state) via input data that triggers an error.	7.5	More Details
CVE-2020-6077	An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages, the implementation does not properly keep track of the available data in the message, possibly leading to an out-of-bounds read that would result in a denial of service. An attacker can send an mDNS message to trigger this vulnerability.	7.5	More Details
CVE-2019-17185	In FreeRADIUS 3.0.x before 3.0.20, the EAP-pwd module used a global OpenSSL BN_CTX instance to handle all handshakes. This mean multiple threads use the same BN_CTX instance concurrently, resulting in crashes when concurrent EAP-pwd handshakes are initiated. This can be abused by an adversary as a Denial-of-Service (DoS) attack.	7.5	More Details
CVE-2019-16528	An issue was discovered in the AbuseFilter extension for MediaWiki. includes/special/SpecialAbuseLog.php allows attackers to obtain sensitive information, such as deleted/suppressed usernames and summaries, from AbuseLog revision data. This affects REL1_32 and REL1_33.	7.5	More Details
CVE-2020-6078	An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages in mdns_recv, the return value of the mdns_read_header function is not checked, leading to an uninitialized variable usage that eventually results in a null pointer dereference, leading to service crash. An attacker can send a series of mDNS messages to trigger this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6079	An exploitable denial-of-service vulnerability exists in the resource allocation handling of Videolabs libmicrodns 0.1.0. When encountering errors while parsing mDNS messages, some allocated data is not freed, possibly leading to a denial-of-service condition via resource exhaustion. An attacker can send one mDNS message repeatedly to trigger this vulnerability through decoding of the domain name performed by rr_decode.	7.5	More Details
CVE-2019-20551	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via a Class 0 Type Message. The Samsung ID is SVE-2019-14941 (October 2019).	7.5	More Details
CVE-2020-6979	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a hard-coded cryptographic key, increasing the possibility that confidential data can be recovered.	7.5	More Details
CVE-2020-10593	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (memory leak), aka TROVE-2020-004. This occurs in circpad_setup_machine_on_circ because a circuit-padding machine can be negotiated twice on the same circuit.	7.5	More Details
CVE-2020-8136	Prototype pollution vulnerability in fastify-multipart < 1.0.5 allows an attacker to crash fastify applications parsing multipart requests by sending a specially crafted request.	7.5	More Details
CVE-2020-6997	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, sensitive information is transmitted over some web applications in cleartext.	7.5	More Details
CVE-2020-7001	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, the affected products use a weak cryptographic algorithm, which may allow confidential information to be disclosed.	7.5	More Details
CVE-2020-8984	lib/NSSDropbox.php in ZendTo prior to 5.22-2 Beta allowed IP address spoofing via the X-Forwarded-For header.	7.5	More Details
CVE-2020-9425	An issue was discovered in includes/head.inc.php in rConfig before 3.9.4. An unauthenticated attacker can retrieve saved cleartext credentials via a GET request to settings.php. Because the application was not exiting after a redirect is applied, the rest of the page still executed, resulting in the disclosure of cleartext credentials in the response.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10792	openITCOCKPIT through 3.7.2 allows remote attackers to configure the self::DEVELOPMENT or self::STAGING option by placing a hostname containing "dev" or "staging" in the HTTP Host header.	7.5	More Details
CVE-2019-19324	Xmidt cjwt through 1.0.1 before 2019-11-25 maps unsupported algorithms to alg=none, which sometimes leads to untrusted accidental JWT acceptance.	7.5	More Details
CVE-2019-15075	An issue was discovered in iNextrix ASTPP before 4.0.1. web_interface/astpp/application/config/config.php does not have strong random keys, as demonstrated by use of the 8YSDaBtDHAB3EQkxPAyTz2I5DttzA9uR private key and the r)fddEw232f encryption key.	7.5	More Details
CVE-2019-20552	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via an RCS call. The Samsung ID is SVE-2019-15035 (October 2019).	7.5	More Details
CVE-2019-14855	A flaw was found in the way certificate signatures could be forged using collisions found in the SHA-1 algorithm. An attacker could use this weakness to create forged certificate signatures. This issue affects GnuPG versions before 2.2.18.	7.5	More Details
CVE-2020-10592	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (CPU consumption), aka TROVE-2020-002.	7.5	More Details
CVE-2019-20620	An issue was discovered on Samsung mobile devices with P(9.0) software. The Settings application allows unauthenticated changes. The Samsung IDs are SVE-2019-13814, SVE-2019-13815 (March 2019).	7.5	More Details
CVE-2020-10854	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Kernel stack addresses are leaked to userspace. The Samsung ID is SVE-2019-16161 (January 2020).	7.5	More Details
CVE-2020-10931	Memcached 1.6.x before 1.6.2 allows remote attackers to cause a denial of service (daemon crash) via a crafted binary protocol header to try_read_command_binary in memcached.c.	7.5	More Details
CVE-2020-10831	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can trigger an update to arbitrary touch-screen firmware. The Samsung ID is SVE-2019-16013 (March 2020).	7.5	More Details
CVE-2020-10875	Motorola FX9500 devices allow remote attackers to conduct absolute path traversal attacks, as demonstrated by PL/SQL Server Pages files such as /include/viewtagdb.psp.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8859	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of ELOG Electronic Logbook 3.1.4-283534d. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of HTTP parameters. A crafted request can trigger the dereference of a null pointer. An attacker can leverage this vulnerability to create a denial-of-service condition. Was ZDI-CAN-10115.	7.5	More Details
CVE-2020-10874	Motorola FX9500 devices allow remote attackers to read database files.	7.5	More Details
CVE-2019-6558	In Auto-Maskin RP210E Versions 3.7 and prior, DCU210E Versions 3.7 and prior and Marine Observer Pro (Android App), the software contains a mechanism for users to recover or change their passwords without knowing the original password, but the mechanism is weak.	7.5	More Details
CVE-2019-20599	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. Voice Assistant mishandles the notification audibility of a secured app. The Samsung ID is SVE-2018-13326 (May 2019).	7.5	More Details
CVE-2020-7478	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory exists in IGSS (Versions 14 and prior using the service: IGSSupdate), which could allow a remote unauthenticated attacker to read arbitrary files from the IGSS server PC on an unrestricted or shared network when the IGSS Update Service is enabled.	7.5	More Details
CVE-2019-20601	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos7570, 7580, 7870, 7880, and 8890 chipsets) software. RKP memory corruption causes an arbitrary write to protected memory. The Samsung ID is SVE-2019-13921-2 (May 2019).	7.5	More Details
CVE-2019-20564	An issue was discovered on Samsung mobile devices with any (before October 2019 for S9 or Note9) software. Attackers can manipulate the IMEI. The Samsung ID is SVE-2019-15435 (October 2019).	7.5	More Details
CVE-2020-7477	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Quantum Ethernet Network module 140NOE771x1 (Versions 7.0 and prior), Quantum processors with integrated Ethernet – 140CPU65xxxxx (all Versions), and Premium processors with integrated Ethernet (all Versions), which could cause a Denial of Service when sending a specially crafted command over Modbus.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10833	An issue was discovered on Samsung mobile devices with Q(10.0) software. The DeX Lockscreen allows attackers to access the quick panel and notifications. The Samsung ID is SVE-2019-16532 (March 2020).	7.5	More Details
CVE-2019-4553	IBM API Connect V5.0.0.0 through 5.0.8.7iFix3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165958.	7.5	More Details
CVE-2020-6983	In Moxa PT-7528 series firmware, Version 4.0 or lower, and PT-7828 series firmware, Version 3.9 or lower, the affected products use a hard-coded cryptographic key, which increases the possibility that confidential data can be recovered.	7.5	More Details
CVE-2019-20577	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos chipsets) software. The MALI GPU Driver allows a kernel panic. The Samsung ID is SVE-2019-14372 (August 2019).	7.5	More Details
CVE-2019-20603	An issue was discovered on Samsung mobile devices with N(7.x), O(8.0), and P(9.0) (Qualcomm chipsets) software. The ESECOMM Trustlet has a NULL pointer dereference. The Samsung ID is SVE-2019-13950 (May 2019).	7.5	More Details
CVE-2019-20604	An issue was discovered on Samsung mobile devices with O(8.x) software. Attackers can disable Gallery permanently. The Samsung ID is SVE-2019-14031 (May 2019).	7.5	More Details
CVE-2019-20608	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. An attacker can use Emergency mode to disable features. The Samsung IDs are SVE-2018-13164, SVE-2018-13165 (April 2019).	7.5	More Details
CVE-2019-18242	In Moxa ioLogik 2500 series firmware, Version 3.0 or lower, and IOxpress configuration utility, Version 2.3.0 or lower, frequent and multiple requests for short-term use may cause the web server to fail.	7.5	More Details
CVE-2019-20612	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) (Broadcom Wi-Fi, and SEC Wi-Fi chipsets) software. Wi-Fi allows a denial of service via TCP SYN packets. The Samsung ID is SVE-2018-13162 (March 2019).	7.5	More Details
CVE-2019-20570	An issue was discovered on Samsung mobile devices with P(9.0), O(8.0), and N(7.1) software. Attackers can bypass Factory Reset Protection (FRP) via Smart Switch. The Samsung ID is SVE-2019-15138 (September 2019).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20614	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. Allshare allows attackers to access sensitive information. The Samsung ID is SVE-2018-13453 (March 2019).	7.5	More Details
CVE-2019-20618	An issue was discovered on Samsung mobile devices with P(9.0) software. The Pin Window feature allows unauthenticated unpinning of an app. The Samsung ID is SVE-2018-13765 (March 2019).	7.5	More Details
CVE-2020-10364	The SSH daemon on MikroTik routers through v6.44.3 could allow remote attackers to generate CPU activity, trigger refusal of new authorized connections, and cause a reboot via connect and write system calls, because of uncontrolled resource management.	7.5	More Details
CVE-2019-20619	An issue was discovered on Samsung mobile devices with P(9.0) software. Secure Startup leaks keyboard suggested words. The Samsung ID is SVE-2019-13773 (March 2019).	7.5	More Details
CVE-2019-20602	An issue was discovered on Samsung mobile devices with N(7.x), O(8.0), and P(9.0) (Qualcomm chipsets) software. The Authnr Trustlet has a NULL pointer dereference. The Samsung ID is SVE-2019-13949 (May 2019).	7.5	More Details
CVE-2019-11939	Golang Facebook Thrift servers would not error upon receiving messages declaring containers of sizes larger than the payload. As a result, malicious clients could send short messages which would result in a large memory allocation, potentially leading to denial of service. This issue affects Facebook Thrift prior to v2020.03.16.00.	7.5	More Details
CVE-2019-20529	In core/doctype/prepared_report/prepared_report.py in Frappe 11 and 12, data files generated with Prepared Report were being stored as public files (no authentication is required to access; having a link is sufficient) instead of private files.	7.5	More Details
CVE-2019-10682	django-nopassword before 5.0.0 stores cleartext secrets in the database.	7.5	More Details
CVE-2019-15654	Comba AC2400 devices are prone to password disclosure via a simple crafted /09/business/upgrade/upcfgAction.php?download=true request to the web management server. The request doesn't require any authentication and will lead to saving the DBconfig.cfg file. At the end of the file, the login information is stored in cleartext.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-15655	D-Link DSL-2875AL devices through 1.00.05 are prone to password disclosure via a simple crafted /romfile.cfg request to the web management server. This request doesn't require any authentication and will lead to saving the configuration file. The password is stored in cleartext.	7.5	More Details
CVE-2019-15656	D-Link DSL-2875AL and DSL-2877AL devices through 1.00.05 are prone to information disclosure via a simple crafted request to index.asp on the web management server because of username_v and password_v variables.	7.5	More Details
CVE-2019-16067	NETSAS Enigma NMS 65.0.0 and prior utilises basic authentication over HTTP for enforcing access control to the web application. The use of weak authentication transmitted over cleartext protocols can allow an attacker to steal username and password combinations by intercepting authentication traffic in transit.	7.5	More Details
CVE-2020-10675	The Library API in buger jsonparser through 2019-12-04 allows attackers to cause a denial of service (infinite loop) via a Delete call.	7.5	More Details
CVE-2019-3762	Data Protection Central versions 1.0, 1.0.1, 18.1, 18.2, and 19.1 contains an Improper Certificate Chain of Trust Vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by obtaining a CA signed certificate from Data Protection Central to impersonate a valid system to compromise the integrity of data.	7.5	More Details
CVE-2019-16063	NETSAS Enigma NMS 65.0.0 and prior does not encrypt sensitive data rendered within web pages. It is possible for an attacker to expose unencrypted sensitive data.	7.5	More Details
CVE-2020-10669	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to authentication bypass on the page /home.jsp. An unauthenticated attacker able to connect to the device's web interface can get a copy of the documents uploaded by any users. NOTE: this is fixed in the latest version.	7.5	More Details
CVE-2019-16108	phpBB 3.2.7 allows adding an arbitrary Cascading Style Sheets (CSS) token sequence to a page through BBCode.	7.5	More Details
CVE-2018-20333	An issue was discovered in ASUSWRT 3.0.0.4.384.20308. An unauthenticated user can request /update_applist.asp to see if a USB device is attached to the router and if there are apps installed on the router.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-20335	An issue was discovered in ASUSWRT 3.0.0.4.384.20308. An unauthenticated user can trigger a DoS of the httpd service via the /APP_Installation.asp?= URI.	7.5	More Details
CVE-2019-18785	SuiteCRM 7.10.x prior to 7.10.21 and 7.11.x prior to 7.11.9 mishandles API access tokens and credentials.	7.5	More Details
CVE-2019-12121	An issue was detected in ONAP Portal through Dublin. By executing a padding oracle attack using the ONAPPORTAL/processSingleSignOn UserId field, an attacker is able to decrypt arbitrary information encrypted with the same symmetric key as UserId. All Portal setups are affected.	7.5	More Details
CVE-2020-9326	BeyondTrust Privilege Management for Windows and Mac (aka PMWM; formerly Avecto Defendpoint) 5.1 through 5.5 before 5.5 SR1 mishandles command-line arguments with PowerShell .ps1 file extensions present, leading to a DefendpointService.exe crash.	7.5	More Details
CVE-2019-15653	Comba AP2600-I devices through A02,0202N00PD2 are prone to password disclosure via an insecure authentication mechanism. The HTML source code of the login page contains values that allow obtaining the username and password. The username are password values are a double md5 of the plaintext real value, i.e., md5(md5(value)).	7.5	More Details
CVE-2020-8470	Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) server contains a vulnerable service DLL file that could allow an attacker to delete any file on the server with SYSTEM level privileges. Authentication is not required to exploit this vulnerability.	7.5	More Details
CVE-2020-9325	Aquaforest TIFF Server 4.0 allows Unauthenticated Arbitrary File Download.	7.5	More Details
CVE-2020-9324	Aquaforest TIFF Server 4.0 allows Unauthenticated SMB Hash Capture via UNC.	7.5	More Details
CVE-2019-11688	An issue was discovered in ASUSTOR exFAT Driver through 1.0.0.r20. When conducting license validation, exfat.cgi and exfatctl accept any certificate for asustornasapi.asustor.com. In other words, there is Missing SSL Certificate Validation.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9392	An issue was discovered in the pricing-table-by-supsystic plugin before 1.8.2 for WordPress. Because there is no permission check on the ImportJSONTable, createFromTpl, and getJSONExportTable endpoints, unauthenticated users can retrieve pricing table information, create new tables, or import/modify a table.	7.3	More Details
CVE-2019-19034	Zoho ManageEngine Asset Explorer 6.5 does not validate the System Center Configuration Manager (SCCM) database username when dynamically generating a command to schedule scans for SCCM. This allows an attacker to execute arbitrary commands on the AssetExplorer Server with NT AUTHORITY/SYSTEM privileges.	7.2	More Details
CVE-2020-8511	In Artica Pandora FMS through 7.42, Web Admin users can execute arbitrary code by uploading a .php file via the File Repository component, a different issue than CVE-2020-7935 and CVE-2020-8500.	7.2	More Details
CVE-2019-18581	Dell EMC Data Protection Advisor versions 6.3, 6.4, 6.5, 18.2 versions prior to patch 83, and 19.1 versions prior to patch 71 contain a server missing authorization vulnerability in the REST API. A remote authenticated malicious user with administrative privileges may potentially exploit this vulnerability to alter the application's allowable list of OS commands. This may lead to arbitrary OS command execution as the regular user runs the DPA service on the affected system.	7.2	More Details
CVE-2019-18582	Dell EMC Data Protection Advisor versions 6.3, 6.4, 6.5, 18.2 versions prior to patch 83, and 19.1 versions prior to patch 71 contain a server-side template injection vulnerability in the REST API. A remote authenticated malicious user with administrative privileges may potentially exploit this vulnerability to inject malicious report generation scripts in the server. This may lead to OS command execution as the regular user runs the DPA service on the affected system.	7.2	More Details
CVE-2020-10934	Acyba AcyMailing before 6.9.2 mishandles file uploads by admins.	7.2	More Details
CVE-2020-7935	Artica Pandora FMS through 7.42 is vulnerable to remote PHP code execution because of an Unrestricted Upload Of A File With A Dangerous Type issue in the File Manager. An attacker can create a (or use an existing) directory that is externally accessible to store PHP files. The filename and the exact path is known by the attacker, so it is possible to execute PHP code in the context of the application. The vulnerability is exploitable only with Administrator access.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10818	Artica Proxy 4.26 allows remote command execution for an authenticated user via shell metacharacters in the "Modify the hostname" field.	7.2	More Details
CVE-2020-6978	In Honeywell WIN-PAK 4.7.2, Web and prior versions, the affected product is vulnerable due to the usage of old jQuery libraries.	7.2	More Details
CVE-2019-15661	An issue was discovered in Rivet Killer Control Center before 2.1.1352. IOCTL 0x120004 in KfeCo10X64.sys fails to validate parameters, leading to a stack-based buffer overflow, which can lead to code execution or escalation of privileges.	7.2	More Details
CVE-2019-19029	Cloud Native Computing Foundation Harbor prior to 1.8.6 and 1.9.3 allows SQL Injection via user-groups in the VMware Harbor Container Registry for the Pivotal Platform.	7.2	More Details
CVE-2016-11022	NETGEAR Prosafe WC9500 5.1.0.17, WC7600 5.1.0.17, and WC7520 2.5.0.35 devices allow a remote attacker to execute code with root privileges via shell metacharacters in the reqMethod parameter to login_handler.php.	7.2	More Details
CVE-2019-15665	An issue was discovered in Rivet Killer Control Center before 2.1.1352. IOCTL 0x120004 in KfeCo10X64.sys fails to validate an offset passed as a parameter during a memory operation, leading to an arbitrary write primitive that can lead to code execution or escalation of privileges.	7.2	More Details
CVE-2020-10840	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 9610 chipsets) software. There is a kernel pointer leak in the vipx driver. The Samsung ID is SVE-2019-16293 (February 2020).	7.1	More Details
CVE-2020-10597	Delta Industrial Automation DOPSoft, Version 4.00.08.15 and prior. Multiple out-of-bounds read vulnerabilities may be exploited by processing specially crafted project files, which may allow an attacker to read information and/or crash the application.	7.1	More Details
CVE-2020-3264	A vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access and make changes to the system that they are not authorized to make.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20531	An issue was discovered on Samsung mobile devices with P(9.0) (Exynos chipsets) software. The Wi-Fi kernel drivers have an out-of-bounds Read. The Samsung IDs are SVE-2019-15692, SVE-2019-15693 (December 2019).	7.1	More Details
CVE-2019-20600	An issue was discovered on Samsung mobile devices with O(8.0) and P(9.0) (Exynos8890 chipsets) software. A use-after-free occurs in the MALI GPU driver. The Samsung ID is SVE-2019-13921-1 (May 2019).	7.1	More Details
CVE-2020-1707	A vulnerability was found in all openshift/postgresql-apb 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the container openshift/postgresql-apb. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	7.0	More Details
CVE-2020-10843	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (S.LSI chipsets) software. There are race conditions in the hdcp2 driver. The Samsung ID is SVE-2019-16296 (February 2020).	7.0	More Details
CVE-2019-5185	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200. An attacker can send a specially crafted packet to trigger the parsing of this cache file. At 0x1ea28 the extracted state value from the xml file is used as an argument to /etc/config-tools/config_interfaces interface=X1 state= <contents of state node> using sprintf(). The destination buffer sp+0x40 is overflowed with the call to sprintf() for any state values that are greater than 512-len("/etc/config-tools/config_interfaces interface=X1 state=") in length. Later, at 0x1ea08 strcpy() is used to copy the contents of the stack buffer that was overflowed sp+0x40 into sp+0x440. The buffer sp+0x440 is immediately adjacent to sp+0x40 on the stack. Therefore, there is no NULL termination on the buffer sp+0x40 since it overflowed into sp+0x440. The strcpy() will result in invalid memory access. An state value of length 0x3c9 will cause the service to crash.	7.0	More Details
CVE-2020-1709	A vulnerability was found in all openshift/mediawiki 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the openshift/mediawiki. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5186	An exploitable stack buffer overflow vulnerability vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200. An attacker can send a specially crafted packet to trigger the parsing of this cache file.At 0x1eb9c the extracted interface element name from the xml file is used as an argument to /etc/config-tools/config_interfaces interface= <contents of interface element> using sprintf(). The destination buffer sp+0x40 is overflowed with the call to sprintf() for any interface values that are greater than 512-len("/etc/config-tools/config_interfaces interface=") in length. Later, at 0x1ea08 strcpy() is used to copy the contents of the stack buffer that was overflowed sp+0x40 into sp+0x440. The buffer sp+0x440 is immediately adjacent to sp+0x40 on the stack. Therefore, there is no NULL termination on the buffer sp+0x40 since it overflowed into sp+0x440. The strcpy() will result in invalid memory access. An interface value of length 0x3c4 will cause the service to crash.	7.0	More Details
CVE-2020-1705	A vulnerability was found in openshift/template-service-broker-operator in all 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the openshift/template-service-broker-operator. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	7.0	More Details
CVE-2019-19351	An insecure modification vulnerability in the /etc/passwd file was found in the container openshift/jenkins. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. This CVE is specific to the openshift/jenkins-slave-base-rhel7-containera as shipped in Openshift 4 and 3.11.	7.0	More Details
CVE-2019-19355	An insecure modification vulnerability in the /etc/passwd file was found in the openshift/ocp-release-operator-sdk. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. This CVE is specific to the openshift/ansible-operator-container as shipped in Openshift 4.	7.0	More Details
CVE-2019-19345	A vulnerability was found in all openshift/mediawiki-apb 4.x.x versions prior to 4.3.0, where an insecure modification vulnerability in the /etc/passwd file was found in the container openshift/mediawiki-apb. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	7.0	More Details
CVE-2019-20594	An issue was discovered on Samsung mobile devices with O(8.1) and P(9.0) (Exynos chipsets) software. A heap overflow exists in the bootloader. The Samsung ID is SVE-2019-14371 (July 2019).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-16258	The bootloader of the homee Brain Cube V2 through 2.23.0 allows attackers with physical access to gain root access by manipulating the U-Boot environment via the CLI after connecting to the internal UART interface.	6.8	More Details
CVE-2020-10847	An issue was discovered on Samsung mobile devices with P(9.0) (Galaxy S8 and Note8) software. Facial recognition can be spoofed. The Samsung ID is SVE-2019-16614 (February 2020).	6.8	More Details
CVE-2020-10839	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) via a SIM card. The Samsung ID is SVE-2019-16193 (February 2020).	6.8	More Details
CVE-2020-10665	Docker Desktop allows local privilege escalation to NT AUTHORITY\SYSTEM because it mishandles the collection of diagnostics with Administrator privileges, leading to arbitrary DACL permissions overwrites and arbitrary file writes. This affects Docker Desktop Enterprise before 2.1.0.9, Docker Desktop for Windows Stable before 2.2.0.4, and Docker Desktop for Windows Edge before 2.2.2.0.	6.7	More Details
CVE-2020-8871	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.0-47107 . An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the VGA virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-9403.	6.7	More Details
CVE-2020-8873	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the xHCI component. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-10031.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8874	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the xHCI component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-10032.	6.7	More Details
CVE-2020-8140	A code injection in Nextcloud Desktop Client 2.6.2 for macOS allowed to load arbitrary code when starting the client with DYLD_INSERT_LIBRARIES set in the environment.	6.7	More Details
CVE-2020-1796	There is an improper authorization vulnerability in several smartphones. The software incorrectly performs an authorization to certain user, successful exploit could allow a low privilege user to do certain operation which the user are supposed not to do.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8);HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2).	6.6	More Details
CVE-2019-20626	The remote keyless system on Honda HR-V 2017 vehicles sends the same RF signal for each door-open request, which might allow a replay attack.	6.5	More Details
CVE-2020-6426	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2019-14873	In the __multadd function of the newlib libc library, prior to versions 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. This will trigger a null pointer dereference bug in case of a memory allocation failure.	6.5	More Details
CVE-2019-16062	NETSAS Enigma NMS 65.0.0 and prior does not encrypt sensitive data stored within the SQL database. It is possible for an attacker to expose unencrypted sensitive data.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8866	This vulnerability allows remote attackers to create arbitrary files on affected installations of Horde Groupware Webmail Edition 5.2.22. Authentication is required to exploit this vulnerability. The specific flaw exists within add.php. The issue results from the lack of proper validation of user-supplied data, which can allow the upload of arbitrary files. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the www-data user. Was ZDI-CAN-10125.	6.5	More Details
CVE-2020-9345	An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the application doesn't limit the number of opened WebSocket sockets. If a victim visits an attacker-controlled website, this vulnerability can be exploited.	6.5	More Details
CVE-2019-14874	In the __i2b function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. The access of _ x[0] will trigger a null pointer dereference bug in case of a memory allocation failure.	6.5	More Details
CVE-2019-14877	In the __mdiff function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate big integers, however no check is performed to verify if the allocation succeeded or not. The access to _wds and _sign will trigger a null pointer dereference bug in case of a memory allocation failure.	6.5	More Details
CVE-2019-14876	In the __lshift function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. The access to b1 will trigger a null pointer dereference bug in case of a memory allocation failure.	6.5	More Details
CVE-2019-14875	In the __multiply function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. The access of _x[0] will trigger a null pointer dereference bug in case of a memory allocation failure.	6.5	More Details
CVE-2020-10844	An issue was discovered on Samsung mobile devices with O(8.x), P(9.x), and Q(10.0) software. There is an out-of-bounds read vulnerability in media.audio_policy. The Samsung ID is SVE-2019-16333 (February 2020).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9343	An issue was discovered in signotec signoPAD-API/Web (formerly Websocket Pad Server) before 3.1.1 on Windows. It is possible to perform a Denial of Service attack because the implementation doesn't limit the parsing of nested JSON structures. If a victim visits an attacker-controlled website, this vulnerability can be exploited via WebSocket data with a deeply nested JSON array.	6.5	More Details
CVE-2019-14872	The _dtoa_r function of the newlib libc library, prior to version 3.3.0, performs multiple memory allocations without checking their return value. This could result in NULL pointer dereference.	6.5	More Details
CVE-2020-8139	A missing access control check in Nextcloud Server < 18.0.1, < 17.0.4, and < 16.0.9 causes hide-download shares to be downloadable when appending /download to the URL.	6.5	More Details
CVE-2019-12921	In GraphicsMagick before 1.3.32, the text filename component allows remote attackers to read arbitrary files via a crafted image because of TranslateTextEx for SVG.	6.5	More Details
CVE-2019-19486	Local File Inclusion in minPlayCommand.php in Centreon (19.04.4 and below) allows an attacker to traverse paths via a plugin test.	6.5	More Details
CVE-2019-14871	The REENT_CHECK macro (see newlib/libc/include/sys/reent.h) as used by REENT_CHECK_TM, REENT_CHECK_MISC, REENT_CHECK_MP and other newlib macros in versions prior to 3.3.0, does not check for memory allocation problems when the DEBUG flag is unset (as is the case in production firmware builds).	6.5	More Details
CVE-2020-10558	The driving interface of Tesla Model 3 vehicles in any release before 2020.4.10 allows Denial of Service to occur due to improper process separation, which allows attackers to disable the speedometer, web browser, climate controls, turn signal visual and sounds, navigation, autopilot notifications, along with other miscellaneous functions from the main screen.	6.5	More Details
CVE-2019-20609	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can use Smartwatch to view Secure Folder notification content. The Samsung ID is SVE-2019-13899 (April 2019).	6.5	More Details
CVE-2019-12122	An issue was discovered in ONAP Portal through Dublin. By executing a call to ONAPPORTAL/portalApi/loggedinUser, an attacker who possesses a user's cookie may retrieve that user's password from the database. All Portal setups are affected.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10194	cs/service/account/AutoCompleteGal.java in Zimbra zm-mailbox before 8.8.15.p8 allows authenticated users to request any GAL account. This differs from the intended behavior in which the domain of the authenticated user must match the domain of the galsync account in the request.	6.5	More Details
CVE-2020-8138	A missing check for IPv4 nested inside IPv6 in Nextcloud server < 17.0.1, < 16.0.7, and < 15.0.14 allowed a Server-Side Request Forgery (SSRF) vulnerability when subscribing to a malicious calendar URL.	6.5	More Details
CVE-2019-14878	In the __d2b function of the newlib libc library, all versions prior to 3.3.0 (see newlib/libc/stdlib/mprec.c), Balloc is used to allocate a big integer, however no check is performed to verify if the allocation succeeded or not. Accessing _x will trigger a null pointer dereference bug in case of a memory allocation failure.	6.5	More Details
CVE-2019-20546	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Broadcom Wi-Fi chipsets) software. A denial-of-service attack can leverage a shared interface between Broadcom Bluetooth and Broadcom Wi-Fi. The Samsung ID is SVE-2019-15350 (November 2019).	6.5	More Details
CVE-2020-10365	LogicalDoc before 8.3.3 allows SQL Injection. LogicalDoc populates the list of available documents by querying the database. This list could be filtered by modifying some of the parameters. Some of them are not properly sanitized which could allow an authenticated attacker to perform arbitrary queries to the database.	6.5	More Details
CVE-2020-8838	An issue was discovered in Zoho ManageEngine AssetExplorer 6.5. During an upgrade of the Windows agent, it does not validate the source and binary downloaded. This allows an attacker on an adjacent network to execute code with NT AUTHORITY/SYSTEM privileges on the agent machines by providing an arbitrary executable via a man-in-the-middle attack.	6.4	More Details
CVE-2020-10845	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. There is a race condition leading to a use-after-free in MTP. The Samsung ID is SVE-2019-16520 (February 2020).	6.4	More Details
CVE-2020-4205	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.8 could allow an authenticated user to bypass security restrictions, and continue to access the server even after authentication certificates have been revolked. IBM X-Force ID: 174961.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8865	This vulnerability allows remote attackers to execute local PHP files on affected installations of Horde Groupware Webmail Edition 5.2.22. Authentication is required to exploit this vulnerability. The specific flaw exists within edit.php. When parsing the params[template] parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the www-data user. Was ZDI-CAN-10469.	6.3	More Details
CVE-2019-20535	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) software. A connection to a new Bluetooth devices can be established from the lock screen. The Samsung ID is SVE-2019-15533 (December 2019).	6.2	More Details
CVE-2019-20569	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via the status bar. The Samsung ID is SVE-2019-15089 (September 2019).	6.2	More Details
CVE-2019-20554	An issue was discovered on Samsung mobile devices with O(8.x) software. Attackers can bypass Factory Reset Protection (FRP) via an external keyboard. The Samsung ID is SVE-2019-15164 (October 2019).	6.2	More Details
CVE-2020-6802	In Mozilla Bleach before 3.11, a mutation XSS affects users calling bleach.clean with noscript and a raw tag in the allowed/whitelisted tags option.	6.1	More Details
CVE-2019-19336	A cross-site scripting vulnerability was reported in the oVirt-engine's OAuth authorization endpoint before version 4.3.8. URL parameters were included in the HTML response without escaping. This flaw would allow an attacker to craft malicious HTML pages that can run scripts in the context of the user's oVirt session.	6.1	More Details
CVE-2019-20523	ilchCMS 2.1.23 allows XSS via the index.php/partner/index Name parameter.	6.1	More Details
CVE-2019-14882	A vulnerability was found in Moodle 3.7 to 3.7.3, 3.6 to 3.6.7, 3.5 to 3.5.9 and earlier where an open redirect existed in the Lesson edit page.	6.1	More Details
CVE-2019-20524	ilchCMS 2.1.23 allows XSS via the index.php/partner/index Banner parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12365	The Newton application through 10.0.23 for Android allows XSS via an event attribute and arbitrary file loading via a src attribute, if the application has the READ_EXTERNAL_STORAGE permission.	6.1	More Details
CVE-2020-10570	The Telegram application through 5.12 for Android, when Show Popup is enabled, might allow physically proximate attackers to bypass intended restrictions on message reading and message replying. This might be interpreted as a bypass of the passcode feature.	6.1	More Details
CVE-2020-9443	Zulip Desktop before 4.0.3 loaded untrusted content in an Electron webview with web security disabled, which can be exploited for XSS in a number of ways. This especially affects Zulip Desktop 2.3.82.	6.1	More Details
CVE-2019-14884	A vulnerability was found in Moodle 3.7 before 3.73, 3.6 before 3.6.7 and 3.5 before 3.5.9, where a reflected XSS possible from some fatal error messages.	6.1	More Details
CVE-2019-12416	we got reports for 2 injection attacks against the DeltaSpike windowhandler.js. This is only active if a developer selected the ClientSideWindowStrategy which is not the default.	6.1	More Details
CVE-2019-12366	The Nine application through 4.5.3a for Android allows XSS via an event attribute and arbitrary file loading via a src attribute, if the application has the READ_EXTERNAL_STORAGE permission.	6.1	More Details
CVE-2019-12367	The BlueMail application through 1.9.5.36 for Android allows XSS via an event attribute and arbitrary file loading via a src attribute, if the application has the READ_EXTERNAL_STORAGE permission.	6.1	More Details
CVE-2019-4681	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 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: 171734.	6.1	More Details
CVE-2019-20527	Ignite Realtime Openfire 4.4.1 allows XSS via the setup/setup-datasource-standard.jsp serverURL parameter.	6.1	More Details
CVE-2019-14881	A vulnerability was found in moodle 3.7 before 3.7.3, where there is blind XSS reflected in some locations where user email is displayed.	6.1	More Details
CVE-2019-20522	ilchCMS 2.1.23 allows XSS via the index.php/partner/index Link parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-12369	The TypeApp application through 1.9.5.35 for Android allows XSS via an event attribute and arbitrary file loading via a src attribute, if the application has the READ_EXTERNAL_STORAGE permission.	6.1	More Details
CVE-2019-12370	The Spark application through 2.0.2 for Android allows XSS via an event attribute and arbitrary file loading via a src attribute, if the application has the READ_EXTERNAL_STORAGE permission.	6.1	More Details
CVE-2019-20511	ERPNext 11.1.47 allows blog?blog_category= Frame Injection.	6.1	More Details
CVE-2019-20512	Open edX Ironwood.1 allows support/certificates?course_id= reflected XSS.	6.1	More Details
CVE-2019-20528	Ignite Realtime Openfire 4.4.1 allows XSS via the setup/setup-datasource-standard.jsp username parameter.	6.1	More Details
CVE-2019-12368	The Edison Mail application through 1.7.1 for Android allows XSS via an event attribute and arbitrary file loading via a src attribute, if the application has the READ_EXTERNAL_STORAGE permission.	6.1	More Details
CVE-2020-6816	In Mozilla Bleach before 3.12, a mutation XSS in bleach.clean when RCDATA and either svg or math tags are whitelisted and the keyword argument strip=False.	6.1	More Details
CVE-2020-7482	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could cause a Reflective Cross-site Scripting (XSS attack) when using the products' web server.	6.1	More Details
CVE-2019-20514	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the address/ URI.	6.1	More Details
CVE-2019-20526	Ignite Realtime Openfire 4.4.1 allows XSS via the setup/setup-datasource-standard.jsp password parameter.	6.1	More Details
CVE-2019-20525	Ignite Realtime Openfire 4.4.1 allows XSS via the setup/setup-datasource-standard.jsp driver parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-15124	In the MobileFrontend extension for MediaWiki, XSS exists within the edit summary field of the watchlist feed. This affects REL1_31, REL1_32, and REL1_33.	6.1	More Details
CVE-2019-20521	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the api/ URI.	6.1	More Details
CVE-2019-20520	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the api/method/ URI.	6.1	More Details
CVE-2019-20519	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the user/ URI, as demonstrated by a crafted e-mail address.	6.1	More Details
CVE-2019-15539	The proj_doc_edit_page.php Project Documentation feature in MantisBT before 2.21.3 has a stored cross-site scripting (XSS) vulnerability, allowing execution of arbitrary code (if CSP settings permit it) after uploading an attachment with a crafted filename. The code is executed when editing the document's page.	6.1	More Details
CVE-2020-7481	A CWE-79:Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists Andover Continuum (All versions), which could enable a successful Cross-site Scripting (XSS attack) when using the products' web server.	6.1	More Details
CVE-2019-20518	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the project/ URI.	6.1	More Details
CVE-2020-10667	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Stored XSS in /TemplateManager/indexExternalLocation.jsp. The vulnerable parameter is map(template_name). NOTE: this is fixed in the latest version.	6.1	More Details
CVE-2019-20517	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the contact/ URI.	6.1	More Details
CVE-2019-20516	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the blog/ URI.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20515	ERPNext 11.1.47 allows reflected XSS via the PATH_INFO to the addresses/ URI.	6.1	More Details
CVE-2019-15510	ManageEngine_DesktopCentral.exe in Zoho ManageEngine Desktop Central 10 allows HTML injection on the user administration page via the description of a role.	6.1	More Details
CVE-2020-10668	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in /home.jsp. The vulnerable parameter is openSI. NOTE: this is fixed in the latest version.	6.1	More Details
CVE-2020-10670	The web application exposed by the Canon Oce Colorwave 500 4.0.0.0 printer is vulnerable to Reflected XSS in the parameter settingId of the settingDialogContent.jsp page. NOTE: this is fixed in the latest version.	6.1	More Details
CVE-2019-16070	A number of stored Cross-site Scripting (XSS) vulnerabilities were identified in NETSAS Enigma NMS 65.0.0 and prior that could allow a threat actor to inject malicious code directly into the application through web application form inputs.	6.1	More Details
CVE-2019-16069	A number of stored Cross-site Scripting (XSS) vulnerabilities were identified in NETSAS Enigma NMS 65.0.0 and prior that could allow a threat actor to inject malicious code directly into the application through the SNMP protocol.	6.1	More Details
CVE-2019-18860	Squid before 4.9, when certain web browsers are used, mishandles HTML in the host (aka hostname) parameter to cachemgr.cgi.	6.1	More Details
CVE-2020-9344	Subversion ALM for the enterprise before 8.8.2 allows reflected XSS at multiple locations.	6.1	More Details
CVE-2019-20513	Open edX Ironwood.1 allows support/certificates?user= reflected XSS.	6.1	More Details
CVE-2019-13463	An XSS vulnerability in qcopd-shortcode-generator.php in the Simple Link Directory plugin before 7.3.5 for WordPress allows remote attackers to inject arbitrary web script or HTML, because esc_html is not called for the "echo get_the_title()" or "echo $term->name" statement.	6.1	More Details
CVE-2019-13389	RainLoop Webmail before 1.13.0 lacks XSS protection mechanisms such as xlink:href validation, the X-XSS-Protection header, and the Content-Security-Policy header.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19484	Open redirect via parameter ‘p’ in login.php in Centreon (19.04.4 and below) allows an attacker to craft a payload and execute unintended behavior.	6.1	More Details
CVE-2020-10941	Arm Mbed TLS before 2.16.5 allows attackers to obtain sensitive information (an RSA private key) by measuring cache usage during an import.	5.9	More Details
CVE-2019-20485	qemu/qemu_driver.c in libvirt before 6.0.0 mishandles the holding of a monitor job during a query to a guest agent, which allows attackers to cause a denial of service (API blockage).	5.7	More Details
CVE-2020-1744	A flaw was found in keycloak before version 9.0.1. When configuring an Conditional OTP Authentication Flow as a post login flow of an IDP, the failure login events for OTP are not being sent to the brute force protection event queue. So BruteForceProtector does not handle this events.	5.6	More Details
CVE-2020-6976	Delta Industrial Automation CNCSoft ScreenEditor, v1.00.96 and prior. An out-of-bounds read overflow can be exploited when a valid user opens a specially crafted, malicious input file due to the lack of validation.	5.5	More Details
CVE-2020-1878	Huawei smartphone OxfordS-AN00A with versions earlier than 10.0.1.152D(C735E152R3P3),versions earlier than 10.0.1.160(C00E160R4P1) have an improper authentication vulnerability. Authentication to target component is improper when device performs an operation. Attackers exploit this vulnerability to obtain some information by loading malicious application, leading to information leak.	5.5	More Details
CVE-2019-20550	An issue was discovered on Samsung mobile devices with O(8.x) (released in China and India) software. The S Secure app can access the content of a locked app without a password. The Samsung ID is SVE-2019-13805 (October 2019).	5.5	More Details
CVE-2020-10811	An issue was discovered in HDF5 through 1.12.0. A heap-based buffer over-read exists in the function H5O__layout_decode() located in H5Olayout.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2019-20632	An issue was discovered in libgpac.a in GPAC before 0.8.0, as demonstrated by MP4Box. It contains an invalid pointer dereference in gf_odf_delete_descriptor in odf/desc_private.c that can cause a denial of service via a crafted MP4 file.	5.5	More Details
CVE-2020-10810	An issue was discovered in HDF5 through 1.12.0. A NULL pointer dereference exists in the function H5AC_unpin_entry() located in H5AC.c. It allows an attacker to cause Denial of Service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10809	An issue was discovered in HDF5 through 1.12.0. A heap-based buffer overflow exists in the function Decompress() located in decompress.c. It can be triggered by sending a crafted file to the gif2h5 binary. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2019-20628	An issue was discovered in libgpac.a in GPAC before 0.8.0, as demonstrated by MP4Box. It contains a Use-After-Free vulnerability in gf_m2ts_process_pmt in media_tools/mpegts.c that can cause a denial of service via a crafted MP4 file.	5.5	More Details
CVE-2019-20629	An issue was discovered in libgpac.a in GPAC before 0.8.0, as demonstrated by MP4Box. It contains a heap-based buffer over-read in gf_m2ts_process_pmt in media_tools/mpegts.c that can cause a denial of service via a crafted MP4 file.	5.5	More Details
CVE-2020-10846	An issue was discovered on Samsung mobile devices with P(9.x) and Q(10.x) software. Attackers can enable the OEM unlock feature on a KG-enrolled devices, leading to potentially unwanted binaries being downloaded. The Samsung ID is SVE-2019-16554 (February 2020).	5.5	More Details
CVE-2019-20631	An issue was discovered in libgpac.a in GPAC before 0.8.0, as demonstrated by MP4Box. It contains an invalid pointer dereference in gf_list_count in utils/list.c that can cause a denial of service via a crafted MP4 file.	5.5	More Details
CVE-2019-20630	An issue was discovered in libgpac.a in GPAC before 0.8.0, as demonstrated by MP4Box. It contains a heap-based buffer over-read in BS_ReadByte (called from gf_bs_read_bit) in utils/bitstream.c that can cause a denial of service via a crafted MP4 file.	5.5	More Details
CVE-2020-10812	An issue was discovered in HDF5 through 1.12.0. A NULL pointer dereference exists in the function H5F_get_nrefs() located in H5Fquery.c. It allows an attacker to cause Denial of Service.	5.5	More Details
CVE-2019-20543	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via SamsungPay mini. The Samsung ID is SVE-2019-15090 (November 2019).	5.5	More Details
CVE-2020-10870	Zim through 0.72.1 creates temporary directories with predictable names. A malicious user could predict and create Zim's temporary directories and prevent other users from being able to start Zim, resulting in a denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1951	A carefully crafted or corrupt PSD file can cause an infinite loop in Apache Tika's PSDParser in versions 1.0-1.23.	5.5	More Details
CVE-2020-8876	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the IOCTL handler. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-10029.	5.5	More Details
CVE-2020-1950	A carefully crafted or corrupt PSD file can cause excessive memory usage in Apache Tika's PSDParser in versions 1.0-1.23.	5.5	More Details
CVE-2019-20540	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Exynos chipsets) software. There is a buffer over-read and possible information leak in the core touch screen driver. The Samsung ID is SVE-2019-14942 (November 2019).	5.5	More Details
CVE-2020-10385	A stored cross-site scripting (XSS) vulnerability exists in the WPForms Contact Form (aka wpforms-lite) plugin before 1.5.9 for WordPress.	5.4	More Details
CVE-2019-16375	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.11, and Community Edition 5.0.x through 5.0.37 and 6.0.x through 6.0.22. An attacker who is logged in as an agent or customer user with appropriate permissions can create a carefully crafted string containing malicious JavaScript code as an article body. This malicious code is executed when an agent composes an answer to the original article.	5.4	More Details
CVE-2020-10803	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was discovered where malicious code could be used to trigger an XSS attack through retrieving and displaying results (in tbl_get_field.php and libraries/classes/Display/Results.php). The attacker must be able to insert crafted data into certain database tables, which when retrieved (for instance, through the Browse tab) can trigger the XSS attack.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-17276	OnCommand System Manager versions 9.3 prior to 9.3P18 and 9.4 prior to 9.4P2 are susceptible to a cross site scripting vulnerability that could allow an authenticated attacker to inject arbitrary scripts into the SNMP Community Names label field.	5.4	More Details
CVE-2019-20575	An issue was discovered on Samsung mobile devices with P(9.0) software. The WPA3 handshake feature allows a downgrade or dictionary attack. The Samsung ID is SVE-2019-14204 (August 2019).	5.4	More Details
CVE-2020-6425	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.149 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension.	5.4	More Details
CVE-2020-10681	The Filemanager in CMS Made Simple 2.2.13 has stored XSS via a .pxd file, as demonstrated by m1_files[] to admin/moduleinterface.php.	5.4	More Details
CVE-2019-4718	IBM Jazz for Service Management 3.13 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: 172123.	5.4	More Details
CVE-2019-20539	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (Broadcom chipsets) software. An out-of-bounds Read in the Wi-Fi vendor command leads to an information leak. The Samsung ID is SVE-2019-14869 (November 2019).	5.3	More Details
CVE-2019-20580	An issue was discovered on Samsung mobile devices with P(9.0) software. The Motion photo player allows attackers to bypass the Secure Folder feature to view images. The Samsung ID is SVE-2019-14653 (August 2019).	5.3	More Details
CVE-2020-9323	Aquaforest TIFF Server 4.0 allows Unauthenticated File and Directory Enumeration via tiffserver/tssp.aspx.	5.3	More Details
CVE-2020-8497	In Artica Pandora FMS through 7.42, an unauthenticated attacker can read the chat history. The file is in JSON format and it contains user names, user IDs, private messages, and timestamps.	5.3	More Details
CVE-2019-20593	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. Gallery leaks Private Mode thumbnails. The Samsung ID is SVE-2019-14208 (July 2019).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4309	IBM Content Navigator 3.0CD could disclose sensitive information to an unauthenticated user which could be used to aid in further attacks against the system. IBM X-Force ID: 177080.	5.3	More Details
CVE-2019-20624	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. S-Voice leaks keyboard learned words via the lock screen. The Samsung ID is SVE-2018-12981 (February 2019).	5.3	More Details
CVE-2019-18782	SuiteCRM 7.10.x prior to 7.10.21 and 7.11.x prior to 7.11.9 does not correctly implement the .htaccess protection mechanism.	5.3	More Details
CVE-2020-10807	auth_svc in Caldera before 2.6.5 allows authentication bypass (for REST API requests) via a forged "localhost" string in the HTTP Host header.	5.3	More Details
CVE-2019-14883	A vulnerability was found in Moodle 3.6 before 3.6.7 and 3.7 before 3.7.3, where tokens used to fetch inline atachments in email notifications were not disabled when a user's account was no longer active. Note: to access files, a user would need to know the file path, and their token.	5.3	More Details
CVE-2019-20532	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can access the Developer options without authentication. The Samsung ID is SVE-2019-15800 (December 2019).	5.3	More Details
CVE-2020-10660	HashiCorp Vault and Vault Enterprise versions 0.9.0 through 1.3.3 may, under certain circumstances, have an Entity's Group membership inadvertently include Groups the Entity no longer has permissions to. Fixed in 1.3.4.	5.3	More Details
CVE-2020-10853	An issue was discovered on Samsung mobile devices with P(9.0) software. Gallery leaks cached data. The Samsung IDs are SVE-2019-16010, SVE-2019-16011, SVE-2019-16012 (January 2020).	5.3	More Details
CVE-2019-16529	An issue was discovered in the CheckUser extension through 1.35.0 for MediaWiki. Oversighted edit summaries are still visible in CheckUser results in violation of MediaWiki's permissions model.	5.3	More Details
CVE-2020-9359	KDE Okular before 1.10.0 allows code execution via an action link in a PDF document.	5.3	More Details
CVE-2019-20616	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. Gallery leaks a thumbnail of Private Mode content. The Samsung ID is SVE-2018-13563 (March 2019).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10834	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can view notifications on the lock screen via Routines. The Samsung ID is SVE-2019-15074 (February 2020).	5.3	More Details
CVE-2020-10942	In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow attackers to trigger kernel stack corruption via crafted system calls.	5.3	More Details
CVE-2019-20555	An issue was discovered on Samsung mobile devices with N(7.x) software. The Gallery app allows attackers to view all pictures of a locked device. The Samsung ID is SVE-2019-15189 (October 2019).	5.3	More Details
CVE-2019-20547	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) software. Data may leak via a Bluetooth debug command. The Samsung ID is SVE-2019-15398 (November 2019).	5.3	More Details
CVE-2020-10871	In OpenWrt LuCI git-20.x, remote unauthenticated attackers can retrieve the list of installed packages and services. NOTE: the vendor disputes the significance of this report because, for instances reachable by an unauthenticated actor, the same information is available in other (more complex) ways, and there is no plan to restrict the information further	5.3	More Details
CVE-2019-20617	An issue was discovered on Samsung mobile devices with P(9.0) software. Secure Folder leaks preview data of recent apps. The Samsung ID is SVE-2018-13764 (March 2019).	5.3	More Details
CVE-2020-5252	The command-line "safety" package for Python has a potential security issue. There are two Python characteristics that allow malicious code to “poison-pill” command-line Safety package detection routines by disguising, or obfuscating, other malicious or non-secure packages. This vulnerability is considered to be of low severity because the attack makes use of an existing Python condition, not the Safety tool itself. This can happen if: You are running Safety in a Python environment that you don’t trust. You are running Safety from the same Python environment where you have your dependencies installed. Dependency packages are being installed arbitrarily or without proper verification. Users can mitigate this issue by doing any of the following: Perform a static analysis by installing Docker and running the Safety Docker image: $ docker run --rm -it pyupio/safety check -r requirements.txt Run Safety against a static dependencies list, such as the requirements.txt file, in a separate, clean Python environment. Run Safety from a Continuous Integration pipeline. Use PyUp.io, which runs Safety in a controlled environment and checks Python for dependencies without any need to install them. Use PyUp's Online Requirements Checker.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19026	Cloud Native Computing Foundation Harbor prior to 1.8.6 and 1.9.3 allows SQL Injection via project quotas in the VMware Harbor Container Registry for the Pivotal Platform.	4.9	More Details
CVE-2020-4203	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.8 could potentially disclose highly sensitive information to a privileged user due to improper access controls. IBM X-Force ID: 174956.	4.9	More Details
CVE-2019-16010	A vulnerability in the web UI of the Cisco SD-WAN vManage software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the vManage software. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	4.8	More Details
CVE-2020-10820	Nagios XI 5.6.11 allows XSS via the includes/components/ldap_ad_integration/ password parameter.	4.8	More Details
CVE-2020-10821	Nagios XI 5.6.11 allows XSS via the account/main.php theme parameter.	4.8	More Details
CVE-2020-7256	Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update allows attackers to unspecified impact via unspecified vectors.	4.8	More Details
CVE-2020-10819	Nagios XI 5.6.11 allows XSS via the includes/components/ldap_ad_integration/ username parameter.	4.8	More Details
CVE-2020-7258	Cross site scripting vulnerability in McAfee Network Security Management (NSM) Prior to 9.1 update 6 Mar 2020 Update allows attackers to unspecified impact via unspecified vectors.	4.8	More Details
CVE-2019-10146	A Reflected Cross Site Scripting flaw was found in all pki-core 10.x.x versions module from the pki-core server due to the CA Agent Service not properly sanitizing the certificate request page. An attacker could inject a specially crafted value that will be executed on the victim's browser.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9759	A Vulnerability of LG Electronic web OS TV Emulator could allow an attacker to escalate privileges and overwrite certain files. This vulnerability is due to wrong environment setting. An attacker could exploit this vulnerability through crafted configuration files and executable files.	4.6	More Details
CVE-2020-10855	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via AppTray. The Samsung ID is SVE-2019-16192 (January 2020).	4.6	More Details
CVE-2020-1793	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8);HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2).	4.6	More Details
CVE-2020-1696	A flaw was found in the all pki-core 10.x.x versions, where Token Processing Service (TPS) where it did not properly sanitize Profile IDs, enabling a Stored Cross-Site Scripting (XSS) vulnerability when the profile ID is printed. An attacker with sufficient permissions could trick an authenticated victim into executing a specially crafted Javascript code.	4.6	More Details
CVE-2019-20615	An issue was discovered on Samsung mobile devices with N(7.x) and O(8.x) software. Attackers can bypass Factory Reset Protection (FRP) via SVoice T&C. The Samsung ID is SVE-2018-13547 (March 2019).	4.6	More Details
CVE-2019-20557	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. Attackers can bypass Factory Reset Protection (FRP) via a SIM card by blocking the PUK code. The Samsung ID is SVE-2019-15262 (October 2019).	4.6	More Details
CVE-2019-10178	It was found that the Token Processing Service (TPS) did not properly sanitize the Token IDs from the "Activity" page, enabling a Stored Cross Site Scripting (XSS) vulnerability. An unauthenticated attacker could trick an authenticated victim into creating a specially crafted activity, which would execute arbitrary JavaScript code when viewed in a browser. All versions of pki-core are believed to be vulnerable.	4.6	More Details
CVE-2020-1794	There is an improper authentication vulnerability in several smartphones. The applock does not perform a sufficient authentication in certain scenarios, successful exploit could allow the attacker to gain certain data of the application which is locked. Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8);HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2).	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8872	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.1-47117. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the xHCI component. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the hypervisor. Was ZDI-CAN-9428.	4.4	More Details
CVE-2019-19335	During installation of an OpenShift 4 cluster, the `openshift-install` command line tool creates an `auth` directory, with `kubeconfig` and `kubeadmin-password` files. Both files contain credentials used to authenticate to the OpenShift API server, and are incorrectly assigned word-readable permissions. ose-installer as shipped in Openshift 4.2 is vulnerable.	4.4	More Details
CVE-2020-4199	IBM Tivoli Netcool/OMNIbus 8.1.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 174910.	4.3	More Details
CVE-2020-10659	Entrust Entelligence Security Provider (ESP) before 10.0.60 on Windows mishandles errors during SSL Certificate Validation, leading to situations where (for example) a user continues to interact with a web site that has an invalid certificate chain.	4.3	More Details
CVE-2019-10221	A Reflected Cross Site Scripting vulnerability was found in all pki-core 10.x.x versions, where the pki-ca module from the pki-core server. This flaw is caused by missing sanitization of the GET URL parameters. An attacker could abuse this flaw to trick an authenticated user into clicking a specially crafted link which can execute arbitrary code when viewed in a browser.	4.3	More Details
CVE-2019-10179	A vulnerability was found in all pki-core 10.x.x versions, where the Key Recovery Authority (KRA) Agent Service did not properly sanitize recovery request search page, enabling a Reflected Cross Site Scripting (XSS) vulnerability. An attacker could trick an authenticated victim into executing specially crafted Javascript code.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8877	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9624.	4.3	More Details
CVE-2020-8879	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9626.	4.3	More Details
CVE-2019-19677	arxes-tolina 3.0.0 allows User Enumeration.	4.3	More Details
CVE-2020-8883	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of EPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9880.	4.3	More Details
CVE-2020-5267	In ActionView before versions 6.0.2.2 and 5.2.4.2, there is a possible XSS vulnerability in ActionView's JavaScript literal escape helpers. Views that use the `j` or `escape_javascript` methods may be susceptible to XSS attacks. The issue is fixed in versions 6.0.2.2 and 5.2.4.2.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1879	There is an improper integrity checking vulnerability on some huawei products. The software of the affected product has an improper integrity check which may allow an attacker with high privilege to make malicious modifications.Affected product versions include:HEGE-560 versions 1.0.1.21(SP3);HEGE-570 versions 1.0.1.22(SP3);OSCA-550 versions 1.0.1.21(SP3);OSCA-550A versions 1.0.1.21(SP3);OSCA-550AX versions 1.0.1.21(SP3);OSCA-550X versions 1.0.1.21(SP3).	3.9	More Details
CVE-2019-20533	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) (released in China or India) software. The S Secure app can launch masked apps without a password. The Samsung ID is SVE-2019-13996 (December 2019).	3.3	More Details
CVE-2020-1862	There is a double free vulnerability in some Huawei products. A local attacker with low privilege may perform some operations to exploit the vulnerability. Due to doubly freeing memory, successful exploit may cause some service abnormal. Affected product versions include:CampusInsight versions V100R019C00;ManageOne versions 6.5.RC2.B050.	3.3	More Details
CVE-2019-20625	An issue was discovered on Samsung mobile devices with N(7.1) and O(8.x) (Exynos chipsets) software. The ion debugfs driver allows information disclosure. The Samsung ID is SVE-2018-13427 (February 2019).	3.3	More Details
CVE-2019-20623	An issue was discovered on Samsung mobile devices with N(7.1), O(8.x), and P(9.0) software. Gallery has uninitialized memory disclosure. The Samsung ID is SVE-2018-13060 (February 2019).	3.3	More Details
CVE-2019-15664	An issue was discovered in Rivet Killer Control Center before 2.1.1352. IOCTL 0x120404 in KfeCo10X64.sys fails to validate an offset passed as a parameter during a memory operation, leading to an out-of-bounds read that can be used as part of a chain to escalate privileges (issue 2 of 2).	2.7	More Details
CVE-2019-15663	An issue was discovered in Rivet Killer Control Center before 2.1.1352. IOCTL 0x120404 in KfeCo10X64.sys fails to validate an offset passed as a parameter during a memory operation, leading to an out-of-bounds read that can be used as part of a chain to escalate privileges (issue 1 of 2).	2.7	More Details
CVE-2019-15662	An issue was discovered in Rivet Killer Control Center before 2.1.1352. IOCTL 0x120444 in KfeCo10X64.sys fails to validate an offset passed as a parameter during a memory operation, leading to an arbitrary read primitive that can be used as part of a chain to escalate privileges.	2.7	More Details
CVE-2019-19964	On NETGEAR GS728TPS devices through 5.3.0.35, a remote attacker having network connectivity to the web-administration panel can access part of the web panel, bypassing authentication.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20598	An issue was discovered on Samsung mobile devices with O(8.x) software. Bixby leaks the keyboard's learned words, and the clipboard contents, via the lock screen. The Samsung IDs are SVE-2018-12896, SVE-2018-12897 (May 2019).	2.4	More Details
CVE-2020-1795	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations.Affected product versions include:HUAWEI Mate 20 versions Versions earlier than 10.0.0.188(C00E74R3P8);HUAWEI Mate 30 Pro versions Versions earlier than 10.0.0.203(C00E202R7P2).	2.4	More Details
CVE-2019-20534	An issue was discovered on Samsung mobile devices with P(9.0) software. Attackers can view home-screen wallpaper by adjusting the brightness of a locked screen. The Samsung ID is SVE-2019-15540 (December 2019).	2.4	More Details
CVE-2019-20579	An issue was discovered on Samsung mobile devices with N(7.x), O(8.x), and P(9.0) software. Gallery allows attackers to enable Location information sharing from the lock screen. The Samsung ID is SVE-2019-14462 (August 2019).	2.4	More Details
CVE-2020-10830	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can view notifications by entering many PINs in Lockdown mode. The Samsung ID is SVE-2019-16590 (March 2020).	2.4	More Details
CVE-2019-20559	An issue was discovered on Samsung mobile devices with P(9.0) software. Gallery allows viewing of photos on the lock screen. The Samsung ID is SVE-2019-15055 (October 2019).	2.4	More Details
CVE-2019-20595	An issue was discovered on Samsung mobile devices with P(9.0) software. Quick Panel allows enabling or disabling the Bluetooth stack without authentication. The Samsung ID is SVE-2019-14545 (July 2019).	2.4	More Details
CVE-2019-19347	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none	N/A	More Details
CVE-2019-20510	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-13456. Reason: This candidate is a duplicate of CVE-2019-13456. Notes: All CVE users should reference CVE-2019-13456 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-5104	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-9013. Reason: This candidate is a duplicate of CVE-2019-9013. Notes: All CVE users should reference CVE-2019-9013 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details