SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 December 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-2020-26829	SAP NetWeaver AS JAVA (P2P Cluster Communication), versions - 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows arbitrary connections from processes because of missing authentication check, that are outside the cluster and even outside the network segment dedicated for the internal cluster communication. As result, an unauthenticated attacker can invoke certain functions that would otherwise be restricted to system administrators only, including access to system administration functions or shutting down the system completely.	10.0	More Details
CVE-2020-27127	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27132	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details
CVE-2020-27133	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details
CVE-2020-27134	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information. For more information about these vulnerabilities, see the Details section of this advisory.	9.9	More Details
CVE-2020-24336	An issue was discovered in Contiki through 3.0 and Contiki-NG through 4.5. The code for parsing Type A domain name answers in ip64-dns64.c doesn't verify whether the address in the answer's length is sane. Therefore, when copying an address of an arbitrary length, a buffer overflow can occur. This bug can be exploited whenever NAT64 is enabled.	9.8	More Details
CVE-2020-14244	A vulnerability in the MIME message handling of the Domino server (versions 9 and 10) could potentially be exploited by an unauthenticated attacker resulting in a stack buffer overflow. This could allow a remote attacker to crash the server or inject code into the system which would execute with the privileges of the server.	9.8	More Details
CVE-2020-25175	GE Healthcare Imaging and Ultrasound Products may allow specific credentials to be exposed during transport over the network.	9.8	More Details
CVE-2020-35378	SQL Injection in the login page in Online Bus Ticket Reservation 1.0 allows attackers to execute arbitrary SQL commands and bypass authentication via the username and password fields.	9.8	More Details
CVE-2020-14268	A vulnerability in the MIME message handling of the Notes client (versions 9 and 10) could potentially be exploited by an unauthenticated attacker resulting in a stack buffer overflow. This could allow a remote attacker to crash the client or inject code into the system which would execute with the privileges of the client.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29227	An issue was discovered in Car Rental Management System 1.0. An unauthenticated user can perform a file inclusion attack against the /index.php file with a partial filename in the "page" parameter, to cause local file inclusion resulting in code execution.	9.8	More Details
CVE-2020-35338	The Web Administrative Interface in Mobile Viewpoint Wireless Multiplex Terminal (WMT) Playout Server 20.2.8 and earlier has a default account with a password of "pokon."	9.8	More Details
CVE-2020-5639	Directory traversal vulnerability in FileZen versions from V3.0.0 to V4.2.2 allows remote attackers to upload an arbitrary file in a specific directory via unspecified vectors. As a result, an arbitrary OS command may be executed.	9.8	More Details
CVE-2020-29563	An issue was discovered on Western Digital My Cloud OS 5 devices before 5.07.118. A NAS Admin authentication bypass vulnerability could allow an unauthenticated user to gain access to the device.	9.8	More Details
CVE-2020-25112	An issue was discovered in the IPv6 stack in Contiki through 3.0. There are inconsistent checks for IPv6 header extension lengths. This leads to Denial-of-Service and potential Remote Code Execution via a crafted ICMPv6 echo packet.	9.8	More Details
CVE-2020-25111	An issue was discovered in the IPv6 stack in Contiki through 3.0. There is an insufficient check for the IPv6 header length. This leads to Denial-of-Service and potential Remote Code Execution via a crafted ICMPv6 echo packet.	9.8	More Details
CVE-2020-25110	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. The length byte of a domain name in a DNS query/response is not checked, and is used for internal memory operations. This may lead to successful Denial-of-Service, and possibly Remote Code Execution.	9.8	More Details
CVE-2020-25109	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. The number of DNS queries/responses (set in a DNS header) is not checked against the data present. This may lead to successful Denial-of-Service, and possibly Remote Code Execution.	9.8	More Details
CVE-2020-25108	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. The DNS response data length is not checked (it can be set to an arbitrary value from a packet). This may lead to successful Denial-of-Service, and possibly Remote Code Execution.	9.8	More Details
CVE-2020-25179	GE Healthcare Imaging and Ultrasound Products may allow specific credentials to be exposed during transport over the network.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20136	QuantConnect Lean versions from 2.3.0.0 to 2.4.0.1 are affected by an insecure deserialization vulnerability due to insecure configuration of TypeNameHandling property in Json.NET library.	9.8	More Details
CVE-2020-24338	An issue was discovered in picoTCP through 1.7.0. The DNS domain name record decompression functionality in pico_dns_decompress_name() in pico_dns_common.c does not validate the compression pointer offset values with respect to the actual data present in a DNS response packet, causing out-of-bounds writes that lead to Denial-of-Service and Remote Code Execution.	9.8	More Details
CVE-2020-0457	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-170367562	9.8	More Details
CVE-2020-35466	The Blackfire Docker image through 2020-12-14 contains a blank password for the root user. Systems deployed using affected versions of the Blackfire container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35464	Version 1.3.0 of the Weave Cloud Agent Docker image contains a blank password for the root user. Systems deployed using affected versions of the Weave Cloud Agent container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35463	Version 1.0.0 of the Instana Dynamic APM Docker image contains a blank password for the root user. Systems deployed using affected versions of the Instana Dynamic APM container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-35462	Version 3.16.0 of the CoScale agent Docker image contains a blank password for the root user. Systems deployed using affected versions of the CoScale agent container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-27068	Product: AndroidVersions: Android kernelAndroid ID: A-127973231References: Upstream kernel	9.8	More Details
CVE-2020-4747	IBM Connect:Direct for UNIX 6.1.0, 6.0.0, 4.3.0, and 4.2.0 can allow a local or remote user to obtain an authenticated CLI session due to improper authentication methods. IBM X-Force ID: 188516.	9.8	More Details
CVE-2020-0456	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-170378843	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0455	There is a possible out of bounds write due to a missing bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-170372514	9.8	More Details
CVE-2020-20184	GateOne allows remote attackers to execute arbitrary commands via shell metacharacters in the port field when attempting an SSH connection.	9.8	More Details
CVE-2020-25228	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). A service available on port 10005/tcp of the affected devices could allow complete access to all services without authorization. An attacker could gain full control over an affected device, if he has access to this service. The system manual recommends to protect access to this port.	9.8	More Details
CVE-2020-20189	SQL Injection vulnerability in NewPK 1.1 via the title parameter to admin\newpost.php.	9.8	More Details
CVE-2020-8257	Improper privilege management on services run by Citrix Gateway Plug-in for Windows, versions before and including 13.0-61.48 and 12.1-58.15, lead to privilege escalation attacks	9.8	More Details
CVE-2020-29511	The encoding/xml package in Go (all versions) does not correctly preserve the semantics of element namespace prefixes during tokenization round-trips, which allows an attacker to craft inputs that behave in conflicting ways during different stages of processing in affected downstream applications.	9.8	More Details
CVE-2020-29510	The encoding/xml package in Go versions 1.15 and earlier does not correctly preserve the semantics of directives during tokenization round-trips, which allows an attacker to craft inputs that behave in conflicting ways during different stages of processing in affected downstream applications.	9.8	More Details
CVE-2020-29509	The encoding/xml package in Go (all versions) does not correctly preserve the semantics of attribute namespace prefixes during tokenization round-trips, which allows an attacker to craft inputs that behave in conflicting ways during different stages of processing in affected downstream applications.	9.8	More Details
CVE-2020-25187	Medtronic MyCareLink Smart 25000 all versions are vulnerable when an attacker who gains auth runs a debug command, which is sent to the reader causing heap overflow in the MCL Smart Reader stack. A heap overflow allows attacker to remotely execute code on the MCL Smart Reader, could lead to control of device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25107	An issue was discovered in the DNS implementation in Ethernut in Nut/OS 5.1. There is no check on whether a domain name has '\0' termination. This may lead to successful Denial-of-Service, and possibly Remote Code Execution.	9.8	More Details
CVE-2020-35467	The Docker Docs Docker image through 2020-12-14 contains a blank password for the root user. Systems deployed using affected versions of the Docker Docs container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2020-7540	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause unauthenticated command execution in the controller when sending special HTTP requests.	9.8	More Details
CVE-2020-29591	Versions of the Official registry Docker images through 2.7.0 contain a blank password for the root user. Systems deployed using affected versions of the registry container may allow a remote attacker to achieve root access with a blank password.	9.8	More Details
CVE-2019-7198	This command injection vulnerability allows attackers to execute arbitrary commands in a compromised application. QNAP have already fixed this vulnerability in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later	9.8	More Details
CVE-2020-29667	In Lan ATMService M3 ATM Monitoring System 6.1.0, a remote attacker able to use a default cookie value, such as PHPSESSID=LANIT-IMANAGER, can achieve control over the system because of Insufficient Session Expiration.	9.8	More Details
CVE-2020-19142	iCMS 7 attackers to execute arbitrary OS commands via shell metacharacters in the DB_PREFIX parameter to install/install.php.	9.8	More Details
CVE-2020-19527	iCMS 7.0.14 attackers to execute arbitrary OS commands via shell metacharacters in the DB_NAME parameter to install/install.php.	9.8	More Details
CVE-2020-26201	Askey AP5100W_Dual_SIG_1.01.097 and all prior versions use a weak password at the Operating System (rlx-linux) level. This allows an attacker to gain unauthorized access as an admin or root user to the device Operating System via Telnet or SSH.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29311	Ubilling v1.0.9 allows Remote Command Execution as Root user by executing a malicious command that is injected inside the config file and being triggered by another part of the software.	9.8	More Details
CVE-2020-28215	A CWE-862: Missing Authorization vulnerability exists in Easergy T300 (firmware 2.7 and older), that could cause a wide range of problems, including information exposures, denial of service, and arbitrary code execution when access control checks are not applied consistently.	9.8	More Details
CVE-2020-17530	Forced OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution. Affected software : Apache Struts 2.0.0 - Struts 2.5.25.	9.8	More Details
CVE-2020-24633	There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of access-points or controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below.	9.8	More Details
CVE-2020-24634	An attacker is able to remotely inject arbitrary commands by sending especially crafted packets destined to the PAPI (Aruba Networks AP Management protocol) UDP port (8211) of access-pointsor controllers in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below.	9.8	More Details
CVE-2020-13556	An out-of-bounds write vulnerability exists in the Ethernet/IP server functionality of EIP Stack Group OpENer 2.3 and development commit 8c73bf3. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.8	More Details
CVE-2020-15357	Network Analysis functionality in Askey AP5100W_Dual_SIG_1.01.097 and all prior versions allows remote attackers to execute arbitrary commands via a shell metacharacter in the ping, traceroute, or route options.	9.8	More Details
CVE-2020-28439	This affects all versions of package corenlp-js-prefab. The injection point is located in line 10 in 'index.js.' It depends on a vulnerable package 'corenlp-js-interface.' Vulnerability can be exploited with the following PoC:	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28440	All versions of package corenlp-js-interface are vulnerable to Command Injection via the main function.	9.8	More Details
CVE-2020-29574	An SQL injection vulnerability in the WebAdmin of Cyberoam OS through 2020-12-04 allows unauthenticated attackers to execute arbitrary SQL statements remotely.	9.8	More Details
CVE-2020-19165	PHPSHE 1.7 has SQL injection via the admin.php?mod=user&userlevel_id=1 userlevel_id[] parameter.	9.8	More Details
CVE-2020-27730	In versions 3.0.0-3.9.0, 2.0.0-2.9.0, and 1.0.1, the NGINX Controller Agent does not use absolute paths when calling system utilities.	9.8	More Details
CVE-2020-17438	An issue was discovered in uIP 1.0, as used in Contiki 3.0 and other products. The code that reassembles fragmented packets fails to properly validate the total length of an incoming packet specified in its IP header, as well as the fragmentation offset value specified in the IP header. By crafting a packet with specific values of the IP header length and the fragmentation offset, attackers can write into the .bss section of the program (past the statically allocated buffer that is used for storing the fragmented data) and cause a denial of service in uip_reass() in uip.c, or possibly execute arbitrary code on some target architectures.	9.8	More Details
CVE-2020-17529	Out-of-bounds Write vulnerability in TCP Stack of Apache NuttX (incubating) versions up to and including 9.1.0 and 10.0.0 allows attacker to corrupt memory by supplying and invalid fragmentation offset value specified in the IP header. This is only impacts builds with both CONFIG_EXPERIMENTAL and CONFIG_NET_TCP_REASSEMBLY build flags enabled.	9.8	More Details
CVE-2020-29659	A buffer overflow in the web server of Flexense DupScout Enterprise 10.0.18 allows a remote anonymous attacker to execute code as SYSTEM by overflowing the sid parameter via a GET /settings&sid= attack.	9.8	More Details
CVE-2020-5948	On BIG-IP versions 16.0.0-16.0.0.1, 15.1.0-15.1.0.5, 14.1.0-14.1.2.7, 13.1.0-13.1.3.4, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16608	Notable 1.8.4 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	9.6	More Details
CVE-2020-26831	SAP BusinessObjects BI Platform (Crystal Report), versions - 4.1, 4.2, 4.3, does not sufficiently validate uploaded XML entities during crystal report generation due to missing XML validation, An attacker with basic privileges can inject some arbitrary XML entities leading to internal file disclosure, internal directories disclosure, Server-Side Request Forgery (SSRF) and denial-of-service (DoS).	9.6	More Details
CVE-2020-17132	Microsoft Exchange Remote Code Execution Vulnerability	9.1	More Details
CVE-2020-26838	SAP Business Warehouse, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 782, and SAP BW4HANA, versions - 100, 200 allows an attacker authenticated with (high) developer privileges to submit a crafted request to generate and execute code without requiring any user interaction. It is possible to craft a request which will result in the execution of Operating System commands leading to Code Injection vulnerability which could completely compromise the confidentiality, integrity and availability of the server and any data or other applications running on it.	9.1	More Details
CVE-2020-26837	SAP Solution Manager 7.2 (User Experience Monitoring), version - 7.2, allows an authenticated user to upload a malicious script that can exploit an existing path traversal vulnerability to compromise confidentiality exposing elements of the file system, partially compromise integrity allowing the modification of some configurations and partially compromise availability by making certain services unavailable.	9.1	More Details
CVE-2020-29663	Icinga 2 v2.8.0 through v2.11.7 and v2.12.2 has an issue where revoked certificates due for renewal will automatically be renewed, ignoring the CRL. This issue is fixed in Icinga 2 v2.11.8 and v2.12.3.	9.1	More Details
CVE-2020-24341	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The TCP input data processing function in pico_tcp.c does not validate the length of incoming TCP packets, which leads to an out-of-bounds read when assembling received packets into a data segment, eventually causing Denial-of-Service or an information leak.	9.1	More Details
CVE-2020-17142	Microsoft Exchange Remote Code Execution Vulnerability	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24383	An issue was discovered in FNET through 4.6.4. The code for processing resource records in mDNS queries doesn't check for proper '\0' termination of the resource record name string, leading to an out-of-bounds read, and potentially causing information leak or Denial-or-Service.	9.1	More Details
CVE-2020-17441	An issue was discovered in picoTCP 1.7.0. The code for processing the IPv6 headers does not validate whether the IPv6 payload length field is equal to the actual size of the payload, which leads to an Out-of-Bounds read during the ICMPv6 checksum calculation, resulting in either Denial-of-Service or Information Disclosure. This affects pico_ipv6_extension_headers and pico_checksum_adder (in pico_ipv6.c and pico_frame.c).	9.1	More Details
CVE-2020-17467	An issue was discovered in FNET through 4.6.4. The code for processing the hostname from an LLMNR request doesn't check for '\0' termination. Therefore, the deduced length of the hostname doesn't reflect the correct length of the actual data. This may lead to Information Disclosure in _fnet_llmnr_poll in fnet_llmnr.c during a response to a malicious request of the DNS class IN.	9.1	More Details
CVE-2020-17528	Out-of-bounds Write vulnerability in TCP stack of Apache NuttX (incubating) versions up to and including 9.1.0 and 10.0.0 allows attacker to corrupt memory by supplying arbitrary urgent data pointer offsets within TCP packets including beyond the length of the packet.	9.1	More Details
CVE-2020-29657	In JerryScript 2.3.0, there is an out-of-bounds read in main_print_unhandled_exception in the main-utils.c file.	9.1	More Details
CVE-2020-24445	AEM's Cloud Service offering, as well as version 6.5.6.0 (and below), are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-4633	IBM Resilient SOAR V38.0 could allow a remote attacker to execute arbitrary code on the system, caused by formula injection due to improper input validation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29254	TikiWiki 21.2 allows templates to be edited without CSRF protection. This could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These action include allowing attackers to submit their own code through an authenticated user resulting in local file Inclusion. If an authenticated user who is able to edit TikiWiki templates visits an malicious website, template code can be edited.	8.8	More Details
CVE-2020-0489	In Parse_data of eas_mdls.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution in the media extractor with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151096540	8.8	More Details
CVE-2020-35470	Envoy before 1.16.1 logs an incorrect downstream address because it considers only the directly connected peer, not the information in the proxy protocol header. This affects situations with tcp-proxy as the network filter (not HTTP filters).	8.8	More Details
CVE-2020-35135	The ultimate-category-excluder plugin before 1.2 for WordPress allows ultimate-category-excluder.php CSRF.	8.8	More Details
CVE-2020-29669	In the Macally WIFISD2-2A82 Media and Travel Router 2.000.010, the Guest user is able to reset its own password. This process has a vulnerability which can be used to take over the administrator account and results in shell access. As the admin user may read the /etc/shadow file, the password hashes of each user (including root) can be dumped. The root hash can be cracked easily which results in a complete system compromise.	8.8	More Details
CVE-2020-25499	TOTOLINK A3002RU-V2.0.0 B20190814.1034 allows authenticated remote users to modify the system's 'Run Command'. An attacker can use this functionality to execute arbitrary OS commands on the router.	8.8	More Details
CVE-2020-17158	Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17152	Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability	8.8	More Details
CVE-2019-19289	A vulnerability has been identified in XHQ (All Versions < 6.1). The web interface could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.	8.8	More Details
CVE-2020-25967	The member center function in fastadmin V1.0.0.20200506_beta is vulnerable to a Server-Side Template Injection (SSTI) vulnerability.	8.8	More Details
CVE-2020-8283	An authorised user on a Windows host running Citrix Universal Print Server can perform arbitrary command execution as SYSTEM in CVAD versions before 2009, 1912 LTSR CU1 hotfixes CTX285870 and CTX286120, 7.15 LTSR CU6 hotfix CTX285344 and 7.6 LTSR CU9.	8.8	More Details
CVE-2020-26969	Mozilla developers reported memory safety bugs present in Firefox 82. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83.	8.8	More Details
CVE-2020-8282	A security issue was found in EdgePower 24V/54V firmware v1.7.0 and earlier where, due to missing CSRF protections, an attacker would have been able to perform unauthorized remote code execution.	8.8	More Details
CVE-2020-13526	SQL injection vulnerability exists in the handling of sort parameters in ProcessMaker 3.4.11. A specially crafted HTTP request can cause an SQL injection. The reportTables_Ajax and clientSetupAjax pages are vulnerable to SQL injection in the sort parameter.An attacker can make an authenticated HTTP request to trigger these vulnerabilities.	8.8	More Details
CVE-2020-28860	OpenAssetDigital Asset Management (DAM) through 12.0.19 does not correctly sanitize user supplied input, incorporating it into its SQL queries, allowing for authenticated blind SQL injection.	8.8	More Details
CVE-2020-25183	Medtronic MyCareLink Smart 25000 all versions contain an authentication protocol vuln where the method used to auth between MCL Smart Patient Reader and MyCareLink Smart mobile app is vulnerable to bypass. This vuln allows attacker to use other mobile device or malicious app on smartphone to auth to the patient's Smart Reader, fools the device into thinking its communicating with the actual smart phone application when executed in range of Bluetooth.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17121	Microsoft SharePoint Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-16103	Type confusion in Gallagher Command Centre Server allows a remote attacker to crash the server or possibly cause remote code execution. This issue affects: Gallagher Command Centre 8.30 versions prior to 8.30.1236(MR1); 8.20 versions prior to 8.20.1166(MR3); 8.10 versions prior to 8.10.1211(MR5); version 8.00 and prior versions.	8.8	More Details
CVE-2020-28858	OpenAsset Digital Asset Management (DAM) through 12.0.19 does not correctly verify whether a request made to the application was intentionally made by the user, allowing for cross-site request forgery attacks on all user functions.	8.8	More Details
CVE-2020-35235	vendor/elfinder/php/connector.minimal.php in the secure-file-manager plugin through 2.5 for WordPress loads elFinder code without proper access control. Thus, any authenticated user can run the elFinder upload command to achieve remote code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	8.8	More Details
CVE-2020-5635	Aterm SA3500G firmware versions prior to Ver. 3.5.9 allows an attacker on the adjacent network to send a specially crafted request to a specific URL, which may result in an arbitrary command execution.	8.8	More Details
CVE-2020-26970	When reading SMTP server status codes, Thunderbird writes an integer value to a position on the stack that is intended to contain just one byte. Depending on processor architecture and stack layout, this leads to stack corruption that may be exploitable. This vulnerability affects Thunderbird < 78.5.1.	8.8	More Details
CVE-2020-17143	Microsoft Exchange Server Information Disclosure Vulnerability	8.8	More Details
CVE-2020-26968	Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29479	An issue was discovered in Xen through 4.14.x. In the Ocaml xenstored implementation, the internal representation of the tree has special cases for the root node, because this node has no parent. Unfortunately, permissions were not checked for certain operations on the root node. Unprivileged guests can get and modify permissions, list, and delete the root node. (Deleting the whole xenstore tree is a host-wide denial of service.) Achieving xenstore write access is also possible. All systems using oxenstored are vulnerable. Building and using oxenstored is the default in the upstream Xen distribution, if the Ocaml compiler is available. Systems using C xenstored are not vulnerable.	8.8	More Details
CVE-2020-25759	An issue was discovered on D-Link DSR-250 3.17 devices. Certain functionality in the Unified Services Router web interface could allow an authenticated attacker to execute arbitrary commands, due to a lack of validation of inputs provided in multipart HTTP POST requests.	8.8	More Details
CVE-2020-25758	An issue was discovered on D-Link DSR-250 3.17 devices. Insufficient validation of configuration file checksums could allow a remote, authenticated attacker to inject arbitrary crontab entries into saved configurations before uploading. These entries are executed as root.	8.8	More Details
CVE-2020-25757	A lack of input validation and access controls in Lua CGIs on D-Link DSR VPN routers may result in arbitrary input being passed to system command APIs, resulting in arbitrary command execution with root privileges. This affects DSR-150, DSR-250, DSR-500, and DSR-1000AC with firmware 3.14 and 3.17.	8.8	More Details
CVE-2020-9301	Nolan Ray from Apple Information Security identified a security vulnerability in Spinnaker, all versions prior to version 1.23.4, 1.22.4 or 1.21.5. The vulnerability exists within the handling of SpEL expressions that allows an attacker to read and write arbitrary files within the orca container via authenticated HTTP POST requests.	8.8	More Details
CVE-2020-29569	An issue was discovered in the Linux kernel through 5.10.1, as used with Xen through 4.14.x. The Linux kernel PV block backend expects the kernel thread handler to reset ring->xenblkd to NULL when stopped. However, the handler may not have time to run if the frontend quickly toggles between the states connect and disconnect. As a consequence, the block backend may re-use a pointer after it was freed. A misbehaving guest can trigger a dom0 crash by continuously connecting / disconnecting a block frontend. Privilege escalation and information leaks cannot be ruled out. This only affects systems with a Linux blkback.	8.8	More Details
CVE-2020-26952	Incorrect bookkeeping of functions inlined during JIT compilation could have led to memory corruption and a potentially exploitable crash when handling out-of-memory errors. This vulnerability affects Firefox < 83.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26950	In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2.	8.8	More Details
CVE-2020-35121	An issue was discovered in the Keysight Database Connector plugin before 1.5.0 for Confluence. A malicious user could insert arbitrary JavaScript into saved macro parameters that would execute when a user viewed a page with that instance of the macro.	8.8	More Details
CVE-2020-26959	During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	8.8	More Details
CVE-2020-26960	If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	8.8	More Details
CVE-2020-29481	An issue was discovered in Xen through 4.14.x. Access rights of Xenstore nodes are per domid. Unfortunately, existing granted access rights are not removed when a domain is being destroyed. This means that a new domain created with the same domid will inherit the access rights to Xenstore nodes from the previous domain(s) with the same domid. Because all Xenstore entries of a guest below /local/domain/<domid> are being deleted by Xen tools when a guest is destroyed, only Xenstore entries of other guests still running are affected. For example, a newly created guest domain might be able to read sensitive information that had belonged to a previously existing guest domain. Both Xenstore implementations (C and Ocaml) are vulnerable.	8.8	More Details
CVE-2020-17147	Dynamics CRM Webclient Cross-site Scripting Vulnerability	8.7	More Details
CVE-2020-7560	A CWE-123: Write-what-where Condition vulnerability exists in EcoStruxure™ Control Expert (all versions) and Unity Pro (former name of EcoStruxure™ Control Expert) (all versions), that could cause a crash of the software or unexpected code execution when opening a malicious file in EcoStruxure™ Control Expert software.	8.6	More Details
CVE-2020-17095	Windows Hyper-V Remote Code Execution Vulnerability	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17144	Microsoft Exchange Remote Code Execution Vulnerability	8.4	More Details
CVE-2020-17141	Microsoft Exchange Remote Code Execution Vulnerability	8.4	More Details
CVE-2020-17439	An issue was discovered in uIP 1.0, as used in Contiki 3.0 and other products. The code that parses incoming DNS packets does not validate that the incoming DNS replies match outgoing DNS queries in newdata() in resolv.c. Also, arbitrary DNS replies are parsed if there was any outgoing DNS query with a transaction ID that matches the transaction ID of an incoming reply. Provided that the default DNS cache is quite small (only four records) and that the transaction ID has a very limited set of values that is quite easy to guess, this can lead to DNS cache poisoning.	8.3	More Details
CVE-2020-24334	The code that processes DNS responses in uIP through 1.0, as used in Contiki and Contiki-NG, does not check whether the number of responses specified in the DNS packet header corresponds to the response data available in the DNS packet, leading to an out-of-bounds read and Denial-of-Service in resolv.c.	8.2	More Details
CVE-2020-17437	An issue was discovered in uIP 1.0, as used in Contiki 3.0 and other products. When the Urgent flag is set in a TCP packet, and the stack is configured to ignore the urgent data, the stack attempts to use the value of the Urgent pointer bytes to separate the Urgent data from the normal data, by calculating the offset at which the normal data should be present in the global buffer. However, the length of this offset is not checked; therefore, for large values of the Urgent pointer bytes, the data pointer can point to memory that is way beyond the data buffer in uip_process in uip.c.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7787	This affects all versions of package react-adal. It is possible for a specially crafted JWT token and request URL can cause the nonce, session and refresh values to be incorrectly validated, causing the application to treat an attacker-generated JWT token as authentic. The logical defect is caused by how the nonce, session and refresh values are stored in the browser local storage or session storage. Each key is automatically appended by ||. When the received nonce and session keys are generated, the list of values is stored in the browser storage, separated by ||, with || always appended to the end of the list. Since || will always be the last 2 characters of the stored values, an empty string ("") will always be in the list of the valid values. Therefore, if an empty session parameter is provided in the callback URL, and a specially-crafted JWT token contains an nonce value of "" (empty string), then adal.js will consider the JWT token as authentic.	8.2	More Details
CVE-2020-16104	SQL Injection vulnerability in Enterprise Data Interface of Gallagher Command Centre allows a remote attacker with 'Edit Enterprise Data Interfaces' privilege to execute arbitrary SQL against a third party database if EDI is configured to import data from this database. This issue affects: Gallagher Command Centre 8.30 versions prior to 8.30.1236(MR1); 8.20 versions prior to 8.20.1166(MR3); 8.10 versions prior to 8.10.1211(MR5); 8.00 versions prior to 8.00.1228(MR6); version 7.90 and prior versions.	8.2	More Details
CVE-2020-17140	Windows SMB Information Disclosure Vulnerability	8.1	More Details
CVE-2020-27252	Medtronic MyCareLink Smart 25000 all versions are vulnerable to a race condition in the MCL Smart Patient Reader software update system, which allows unsigned firmware to be uploaded and executed on the Patient Reader. If exploited an attacker could remotely execute code on the MCL Smart Patient Reader device, leading to control of the device.	8.1	More Details
CVE-2020-17118	Microsoft SharePoint Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26830	SAP Solution Manager 7.2 (User Experience Monitoring), version - 7.2, does not perform necessary authorization checks for an authenticated user. Due to inadequate access control, a network attacker authenticated as a regular user can use operations which should be restricted to administrators. These operations can be used to Change the User Experience Monitoring configuration, obtain details about the configured SAP Solution Manager agents, Deploy a malicious User Experience Monitoring script.	8.1	More Details
CVE-2020-17115	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details
CVE-2020-26261	jupyterhub-systemdspawner enables JupyterHub to spawn single-user notebook servers using systemd. In jupyterhub-systemdspawner before version 0.15 user API tokens issued to single-user servers are specified in the environment of systemd units. These tokens are incorrectly accessible to all users. In particular, the-littlest-jupyterhub is affected, which uses systemdspawner by default. This is patched in jupyterhub-systemdspawner v0.15	7.9	More Details
CVE-2020-17122	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17139	Windows Overlay Filter Security Feature Bypass Vulnerability	7.8	More Details
CVE-2020-17137	DirectX Graphics Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17136	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17134	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17092	Windows Network Connections Service Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28219	A CWE-522: Insufficiently Protected Credentials vulnerability exists in EcoStruxure Geo SCADA Expert 2019 (Original release and Monthly Updates to September 2020, from 81.7268.1 to 81.7578.1) and EcoStruxure Geo SCADA Expert 2020 (Original release and Monthly Updates to September 2020, from 83.7551.1 to 83.7578.1), that could cause exposure of credentials to server-side users when web users are logged in to Virtual ViewX.	7.8	More Details
CVE-2020-17128	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17129	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-16963	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17150	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17127	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-8177	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used.	7.8	More Details
CVE-2020-17148	Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17125	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17124	Microsoft PowerPoint Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17123	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16964	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-16959	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-16962	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-16961	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-4829	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user to exploit a vulnerability in the ksu user command to gain root privileges. IBM X-Force ID: 189960.	7.8	More Details
CVE-2020-0475	In createInputConsumer of WindowManagerService.java, there is a possible way to block and intercept input events due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162324374	7.8	More Details
CVE-2020-0478	In extend_frame_lowbd of restoration.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150780418	7.8	More Details
CVE-2020-0479	In callUnchecked of DocumentsProvider.java, there is a possible permissions bypass. This could lead to local escalation of privilege allowing a malicious app to access files available to the DocumentProvider without user permission, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157294893	7.8	More Details
CVE-2020-27614	AnyDesk for macOS versions 6.0.2 and older have a vulnerability in the XPC interface that does not properly validate client requests and allows local privilege escalation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0480	In callUnchecked of DocumentsProvider.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege allowing a caller to copy, move, or delete files accessible to DocumentsProvider with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157320716	7.8	More Details
CVE-2020-0485	In areFunctionsSupported of UsbBackend.java, there is a possible access to tethering from a guest account due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-166125765	7.8	More Details
CVE-2020-0486	In openAssetFileListener of ContactsProvider2.java, there is a possible permission bypass due to an insecure default value. This could lead to local escalation of privilege to change contact data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150857116	7.8	More Details
CVE-2020-27051	In NFA_RwI93WriteMultipleBlocks of nfa_rw_api.cc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157650338	7.8	More Details
CVE-2020-25199	A heap-based buffer overflow vulnerability exists within the WECON LeviStudioU Release Build 2019-09-21 and prior when processing project files. Opening a specially crafted project file could allow an attacker to exploit and execute code under the privileges of the application.	7.8	More Details
CVE-2020-13520	An out of bounds memory corruption vulnerability exists in the way Pixar OpenUSD 20.05 reconstructs paths from binary USD files. A specially crafted malformed file can trigger an out of bounds memory modification which can result in remote code execution. To trigger this vulnerability, victim needs to access an attacker-provided malformed file.	7.8	More Details
CVE-2020-27030	In onCreate of HandleApiCalls.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege that allows an app to set or dismiss the alarm with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150612638	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25712	A flaw was found in xorg-x11-server before 1.20.10. A heap-buffer overflow in XkbSetDeviceInfo may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2020-27044	In restartWrite of Parcel.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157066561	7.8	More Details
CVE-2020-27045	In CE_SendRawFrame of ce_main.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157649398	7.8	More Details
CVE-2020-27048	In RW_SendRawFrame of rw_main.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157650117	7.8	More Details
CVE-2020-27049	In rw_t3t_send_raw_frame of rw_t3t.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157649467	7.8	More Details
CVE-2020-29661	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.	7.8	More Details
CVE-2020-29654	Western Digital Dashboard before 3.2.2.9 allows DLL Hijacking that leads to compromise of the SYSTEM account.	7.8	More Details
CVE-2020-27052	In getLockTaskLaunchMode of ActivityRecord.java, there is a possible way for any app to start in Lock Task Mode due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-158833495	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27054	In onFactoryReset of BluetoothManagerService.java, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-159061926	7.8	More Details
CVE-2020-16960	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-27050	In rw_i93_send_cmd_write_multi_blocks of rw_i93.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157650365	7.8	More Details
CVE-2020-16958	Windows Backup Engine Elevation of Privilege Vulnerability	7.8	More Details
CVE-2020-17156	Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-17159	Visual Studio Code Java Extension Pack Remote Code Execution Vulnerability	7.8	More Details
CVE-2020-10143	Macrium Reflect includes an OpenSSL component that specifies an OPENSSLDIR variable as C:\openssl\. Macrium Reflect contains a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges.	7.8	More Details
CVE-2020-16600	A Use After Free vulnerability exists in Artifex Software, Inc. MuPDF library 1.17.0-rc1 and earlier when a valid page was followed by a page with invalid pixmap dimensions, causing bander - a static - to point to previously freed memory instead of a newband_writer.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0099	In addWindow of WindowManagerService.java, there is a possible window overlay attack due to an insecure default value. This could lead to local escalation of privilege via tapjacking with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-141745510	7.8	More Details
CVE-2020-2049	A local privilege escalation vulnerability exists in Palo Alto Networks Cortex XDR Agent on the Windows platform that allows an authenticated local Windows user to execute programs with SYSTEM privileges. This requires the user to have the privilege to create files in the Windows root directory. This issue impacts: All versions of Cortex XDR Agent 7.1 with content update 149 and earlier versions; All versions of Cortex XDR Agent 7.2 with content update 149 and earlier versions.	7.8	More Details
CVE-2020-0440	In createVirtualDisplay of DisplayManagerService.java, there is a possible way to create a trusted virtual display due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162627132	7.8	More Details
CVE-2020-0458	In SPDIFEncoder::writeBurstBufferBytes and related methods of SPDIFEncoder.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-8.0 Android-8.1Android ID: A-160265164	7.8	More Details
CVE-2020-27786	A flaw was found in the Linux kernel’s implementation of MIDI, where an attacker with a local account and the permissions to issue ioctl commands to midi devices could trigger a use-after-free issue. A write to this specific memory while freed and before use causes the flow of execution to change and possibly allow for memory corruption or privilege escalation. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.8	More Details
CVE-2020-27828	There's a flaw in jasper's jpc encoder in versions prior to 2.0.23. Crafted input provided to jasper by an attacker could cause an arbitrary out-of-bounds write. This could potentially affect data confidentiality, integrity, or application availability.	7.8	More Details
CVE-2020-0466	In do_epoll_ctl and ep_loop_check_proc of eventpoll.c, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-147802478References: Upstream kernel	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0016	In the Broadcom Nexus firmware, there is an insecure default password. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-171413483	7.8	More Details
CVE-2020-35457	GNOME GLib before 2.65.3 has an integer overflow, that might lead to an out-of-bounds write, in g_option_group_add_entries. NOTE: the vendor's position is "Realistically this is not a security issue. The standard pattern is for callers to provide a static list of option entries in a fixed number of calls to g_option_group_add_entries()." The researcher states that this pattern is undocumented	7.8	More Details
CVE-2020-0444	In audit_free_lsm_field of auditfilter.c, there is a possible bad kfree due to a logic error in audit_data_to_entry. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150693166References: Upstream kernel	7.8	More Details
CVE-2020-26249	Red Discord Bot Dashboard is an easy-to-use interactive web dashboard to control your Redbot. In Red Discord Bot before version 0.1.7a an RCE exploit has been discovered. This exploit allows Discord users with specially crafted Server names and Usernames/Nicknames to inject code into the webserver front-end code. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. This high severity exploit has been fixed on version 0.1.7a. There are no workarounds, bot owners must upgrade their relevant packages (Dashboard module and Dashboard webserver) in order to patch this issue.	7.7	More Details
CVE-2020-25234	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3), LOGO! Soft Comfort (All versions < V8.3). The LOGO! program files generated and used by the affected components offer the possibility to save user-defined functions (UDF) in a password protected way. This protection is implemented in the software that displays the information. An attacker could reverse engineer the UDFs directly from stored program files.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26832	SAP AS ABAP (SAP Landscape Transformation), versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 and SAP S4 HANA (SAP Landscape Transformation), versions - 101, 102, 103, 104, 105, allows a high privileged user to execute a RFC function module to which access should be restricted, however due to missing authorization an attacker can get access to some sensitive internal information of vulnerable SAP system or to make vulnerable SAP systems completely unavailable.	7.6	More Details
CVE-2020-13530	A denial-of-service vulnerability exists in the Ethernet/IP server functionality of the EIP Stack Group OpENer 2.3 and development commit 8c73bf3. A large number of network requests in a small span of time can cause the running program to stop. An attacker can send a sequence of requests to trigger this vulnerability.	7.5	More Details
CVE-2020-17440	An issue was discovered in uIP 1.0, as used in Contiki 3.0 and other products. The code that parses incoming DNS packets does not validate that domain names present in the DNS responses have '\0' termination. This results in errors when calculating the offset of the pointer that jumps over domain name bytes in DNS response packets when a name lacks this termination, and eventually leads to dereferencing the pointer at an invalid/arbitrary address, within newdata() and parse_name() in resolv.c.	7.5	More Details
CVE-2020-7542	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	7.5	More Details
CVE-2020-7543	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	7.5	More Details
CVE-2020-25191	Incorrect permissions are set by default for an API entry-point of a specific service, allowing a non-authenticated user to trigger a function that could reboot the CompactRIO (Driver versions prior to 20.5) remotely.	7.5	More Details
CVE-2020-13988	An issue was discovered in Contiki through 3.0. An Integer Overflow exists in the uIP TCP/IP Stack component when parsing TCP MSS options of IPv4 network packets in uip_process in net/ipv4/uip.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13986	An issue was discovered in Contiki through 3.0. An infinite loop exists in the uIP TCP/IP stack component when handling RPL extension headers of IPv6 network packets in rpl_remove_header in net/rpl/rpl-ext-header.c.	7.5	More Details
CVE-2020-13984	An issue was discovered in Contiki through 3.0. An infinite loop exists in the uIP TCP/IP stack component when processing IPv6 extension headers in ext_hdr_options_process in net/ipv6/uip6.c.	7.5	More Details
CVE-2020-5949	On BIG-IP versions 14.0.0-14.0.1 and 13.1.0-13.1.3.4, certain traffic pattern sent to a virtual server configured with an FTP profile can cause the FTP channel to break.	7.5	More Details
CVE-2020-7792	This affects all versions of package mout. The deepFillIn function can be used to 'fill missing properties recursively', while the deepMixIn 'mixes objects into the target object, recursively mixing existing child objects as well'. In both cases, the key used to access the target object recursively is not checked, leading to a Prototype Pollution.	7.5	More Details
CVE-2020-7793	The package ua-parser-js before 0.7.23 are vulnerable to Regular Expression Denial of Service (ReDoS) in multiple regexes (see linked commit for more info).	7.5	More Details
CVE-2020-17443	An issue was discovered in picoTCP 1.7.0. The code for creating an ICMPv6 echo replies doesn't check whether the ICMPv6 echo request packet's size is shorter than 8 bytes. If the size of the incoming ICMPv6 request packet is shorter than this, the operation that calculates the size of the ICMPv6 echo replies has an integer wrap around, leading to memory corruption and, eventually, Denial-of-Service in pico_icmp6_send_echoreply_not_frag in pico_icmp6.c.	7.5	More Details
CVE-2020-13985	An issue was discovered in Contiki through 3.0. A memory corruption vulnerability exists in the uIP TCP/IP stack component when handling RPL extension headers of IPv6 network packets in rpl_remove_header in net/rpl/rpl-ext-header.c.	7.5	More Details
CVE-2020-27508	In two-factor authentication, the system also sending 2fa secret key in response, which enables an intruder to breach the 2fa security.	7.5	More Details
CVE-2020-7791	This affects the package i18n before 2.1.15. Vulnerability arises out of insufficient handling of erroneous language tags in src/i18n/Concrete/TextLocalizer.cs and src/i18n/LocalizedApplication.cs.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27713	In certain configurations on version 13.1.3.4, when a BIG-IP AFM HTTP security profile is applied to a virtual server and the BIG-IP system receives a request with specific characteristics, the connection is reset and the Traffic Management Microkernel (TMM) leaks memory.	7.5	More Details
CVE-2020-17442	An issue was discovered in picoTCP 1.7.0. The code for parsing the hop-by-hop IPv6 extension headers does not validate the bounds of the extension header length value, which may result in Integer Wraparound. Therefore, a crafted extension header length value may cause Denial-of-Service because it affects the loop in which the extension headers are parsed in pico_ipv6_process_hopbyhop() in pico_ipv6.c.	7.5	More Details
CVE-2020-8258	Improper privilege management on services run by Citrix Gateway Plug-in for Windows, versions before and including 13.0-61.48 and 12.1-58.15, allows an attacker to modify arbitrary files.	7.5	More Details
CVE-2020-17444	An issue was discovered in picoTCP 1.7.0. The routine for processing the next header field (and deducing whether the IPv6 extension headers are valid) doesn't check whether the header extension length field would overflow. Therefore, if it wraps around to zero, iterating through the extension headers will not increment the current data pointer. This leads to an infinite loop and Denial-of-Service in pico_ipv6_check_headers_sequence() in pico_ipv6.c.	7.5	More Details
CVE-2020-17445	An issue was discovered in picoTCP 1.7.0. The code for processing the IPv6 destination options does not check for a valid length of the destination options header. This results in an Out-of-Bounds Read, and, depending on the memory protection mechanism, this may result in Denial-of-Service in pico_ipv6_process_destopt() in pico_ipv6.c.	7.5	More Details
CVE-2020-35122	An issue was discovered in the Keysight Database Connector plugin before 1.5.0 for Confluence. A malicious user could bypass the access controls for using a saved database connection profile to submit arbitrary SQL against a saved database connection.	7.5	More Details
CVE-2020-35381	jsonparser 1.0.0 allows attackers to cause a denial of service (panic: runtime error: slice bounds out of range) via a GET call.	7.5	More Details
CVE-2020-35380	GJSON before 1.6.4 allows attackers to cause a denial of service via crafted JSON.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-25195	The length of the input fields of Host Engineering H0-ECOM100, H2-ECOM100, and H4-ECOM100 modules are verified only on the client side when receiving input from the configuration web server, which may allow an attacker to bypass the check and send input to crash the device.	7.5	More Details
CVE-2020-29487	An issue was discovered in Xen XAPI before 2020-12-15. Certain xenstore keys provide feedback from the guest, and are therefore watched by toolstack. Specifically, keys are watched by xenopsd, and data are forwarded via RPC through message-switch to xapi. The watching logic in xenopsd sends one RPC update containing all data, any time any single xenstore key is updated, and therefore has O(N^2) time complexity. Furthermore, message-switch retains recent (currently 128) RPC messages for diagnostic purposes, yielding O(M*N) space complexity. The quantity of memory a single guest can monopolise is bounded by xenstored quota, but the quota is fairly large. It is believed to be in excess of 1G per malicious guest. In practice, this manifests as a host denial of service, either through message-switch thrashing against swap, or OOMing entirely, depending on dom0's configuration. (There are no quotas in xenopsd to limit the quantity of keys that result in RPC traffic.) A buggy or malicious guest can cause unreasonable memory usage in dom0, resulting in a host denial of service. All versions of XAPI are vulnerable. Systems that are not using the XAPI toolstack are not vulnerable.	7.5	More Details
CVE-2020-27055	In isSubmittable and showWarningMessagesIfAppropriate of WifiConfigController.java and WifiConfigController2.java, there is a possible insecure WiFi configuration due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-161378819	7.5	More Details
CVE-2020-27024	In smp_br_state_machine_event of smp_br_main.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure triggered by a malformed Bluetooth packet, with no additional execution privileges needed. User interaction is not needed for exploitation. Bounds Sanitizer mitigates this in the default configuration.Product: AndroidVersions: Android-11Android ID: A-162327732	7.5	More Details
CVE-2020-28442	All versions of package js-data are vulnerable to Prototype Pollution via the deepFillIn function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35471	Envoy before 1.16.1 mishandles dropped and truncated datagrams, as demonstrated by a segmentation fault for a UDP packet size larger than 1500.	7.5	More Details
CVE-2020-0463	In sdp_server_handle_client_req of sdp_server.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure from the bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.0 Android-8.1 Android-9Android ID: A-169342531	7.5	More Details
CVE-2020-0460	In createNameCredentialDialog of CertInstaller.java, there exists the possibility of improperly installed certificates due to a logic error. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-163413737	7.5	More Details
CVE-2020-25235	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). The password used for authentication for the LOGO! Website and the LOGO! Access Tool is sent in a recoverable format. An attacker with access to the network traffic could derive valid logins.	7.5	More Details
CVE-2020-25232	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Due to the usage of an insecure random number generation function and a deprecated cryptographic function, an attacker could extract the key that is used when communicating with an affected device on port 8080/tcp.	7.5	More Details
CVE-2020-25230	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Due to the usage of an outdated cipher mode on port 10005/tcp, an attacker could extract the encryption key from a captured communication with the device.	7.5	More Details
CVE-2020-25229	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). The implemented encryption for communication with affected devices is prone to replay attacks due to the usage of a static key. An attacker could change the password or change the configuration on any affected device if using prepared messages that were generated for another device.	7.5	More Details
CVE-2020-15796	A vulnerability has been identified in SIMATIC ET 200SP Open Controller (incl. SIPLUS variants) (V20.8), SIMATIC S7-1500 Software Controller (V20.8). The web server of the affected products contains a vulnerability that could allow a remote attacker to trigger a denial-of-service condition by sending a specially crafted HTTP request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8286	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.	7.5	More Details
CVE-2020-8285	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.	7.5	More Details
CVE-2020-7537	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium (see security notifications for affected versions), that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller.	7.5	More Details
CVE-2020-8231	Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.	7.5	More Details
CVE-2020-8169	curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure vulnerability that can lead to a partial password being leaked over the network and to the DNS server(s).	7.5	More Details
CVE-2020-20183	Insecure direct object reference vulnerability in Zyxel's P1302-T10 v3 with firmware version 2.00(ABBX.3) and earlier allows attackers to gain privileges and access certain admin pages.	7.5	More Details
CVE-2020-28856	OpenAsset Digital Asset Management (DAM) through 12.0.19 does not correctly determine the HTTP request's originating IP address, allowing attackers to spoof it using X-Forwarded-For in the header, by supplying localhost address such as 127.0.0.1, effectively bypassing all IP address based access controls.	7.5	More Details
CVE-2020-35234	The easy-wp-smtp plugin before 1.4.4 for WordPress allows Administrator account takeover, as exploited in the wild in December 2020. If an attacker can list the wp-content/plugins/easy-wp-smtp/ directory, then they can discover a log file (such as ##########_debug_log.txt) that contains all password-reset links. The attacker can request a reset of the Administrator password and then use a link found there.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24340	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The code that processes DNS responses in pico_mdns_handle_data_as_answers_generic() in pico_mdns.c does not check whether the number of answers/responses specified in a DNS packet header corresponds to the response data available in the packet, leading to an out-of-bounds read, invalid pointer dereference, and Denial-of-Service.	7.5	More Details
CVE-2020-24339	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. The DNS domain name record decompression functionality in pico_dns_decompress_name() in pico_dns_common.c does not validate the compression pointer offset values with respect to the actual data present in a DNS response packet, causing out-of-bounds reads that lead to Denial-of-Service.	7.5	More Details
CVE-2020-24337	An issue was discovered in picoTCP and picoTCP-NG through 1.7.0. When an unsupported TCP option with zero length is provided in an incoming TCP packet, it is possible to cause a Denial-of-Service by achieving an infinite loop in the code that parses TCP options, aka tcp_parse_options() in pico_tcp.c.	7.5	More Details
CVE-2020-17469	An issue was discovered in FNET through 4.6.4. The code for IPv6 fragment reassembly tries to access a previous fragment starting from a network incoming fragment that still doesn't have a reference to the previous one (which supposedly resides in the reassembly list). When faced with an incoming fragment that belongs to a non-empty fragment list, IPv6 reassembly must check that there are no empty holes between the fragments: this leads to an uninitialized pointer dereference in _fnet_ip6_reassembly in fnet_ip6.c, and causes Denial-of-Service.	7.5	More Details
CVE-2020-17468	An issue was discovered in FNET through 4.6.4. The code for processing the hop-by-hop header (in the IPv6 extension headers) doesn't check for a valid length of an extension header, and therefore an out-of-bounds read can occur in _fnet_ip6_ext_header_handler_options in fnet_ip6.c, leading to Denial-of-Service.	7.5	More Details
CVE-2020-7539	A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP.	7.5	More Details
CVE-2020-13987	An issue was discovered in Contiki through 3.0. An Out-of-Bounds Read vulnerability exists in the uIP TCP/IP Stack component when calculating the checksums for IP packets in upper_layer_chksum in net/ipv4/uip.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7536	A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists in Modicon M340 CPUs (BMXP34* versions prior to V3.30) Modicon M340 Communication Ethernet modules (BMXNOE0100 (H) versions prior to V3.4 BMXNOE0110 (H) versions prior to V6.6 BMXNOR0200H all versions), that could cause the device to be unreachable when modifying network parameters over SNMP.	7.5	More Details
CVE-2020-28216	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to read network traffic over HTTP protocol.	7.5	More Details
CVE-2020-12516	Older firmware versions (FW1 up to FW10) of the WAGO PLC family 750-88x and 750-352 are vulnerable for a special denial of service attack.	7.5	More Details
CVE-2020-29655	An injection vulnerability exists in RT-AC88U Download Master before 3.1.0.108. Accessing Main_Login.asp?flag=1&productname=FOOBAR&url=/downloadmaster/task.asp will redirect to the login site, which will show the value of the parameter productname within the title. An attacker might be able to influence the appearance of the login page, aka text injection.	7.5	More Details
CVE-2020-29651	A denial of service via regular expression in the py.path.svnwc component of py (aka python-py) through 1.9.0 could be used by attackers to cause a compute-time denial of service attack by supplying malicious input to the blame functionality.	7.5	More Details
CVE-2020-17096	Windows NTFS Remote Code Execution Vulnerability	7.5	More Details
CVE-2020-26269	In TensorFlow release candidate versions 2.4.0rc*, the general implementation for matching filesystem paths to globbing pattern is vulnerable to an access out of bounds of the array holding the directories. There are multiple invariants and preconditions that are assumed by the parallel implementation of GetMatchingPaths but are not verified by the PRs introducing it (#40861 and #44310). Thus, we are completely rewriting the implementation to fully specify and validate these. This is patched in version 2.4.0. This issue only impacts master branch and the release candidates for TF version 2.4. The final release of the 2.4 release will be patched.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29656	An information disclosure vulnerability exists in RT-AC88U Download Master before 3.1.0.108. A direct access to /downloadmaster/dm_apply.cgi?action_mode=initial&download_type=General&special_cgi=get_language makes it possible to reach "unknown functionality" in a "known to be easy" manner via an unspecified "public exploit."	7.5	More Details
CVE-2020-28086	pass through 1.7.3 has a possibility of using a password for an unintended resource. For exploitation to occur, the user must do a git pull, decrypt a password, and log into a remote service with the password. If an attacker controls the central Git server or one of the other members' machines, and also controls one of the services already in the password store, they can rename one of the password files in the Git repository to something else: pass doesn't correctly verify that the content of a file matches the filename, so a user might be tricked into decrypting the wrong password and sending that to a service that the attacker controls. NOTE: for environments in which this threat model is of concern, signing commits can be a solution.	7.5	More Details
CVE-2020-28217	A CWE-311: Missing Encryption of Sensitive Data vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to read network traffic over HTTP protocol.	7.5	More Details
CVE-2020-7535	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of information when sending a specially crafted request to the controller over HTTP.	7.5	More Details
CVE-2020-17002	Azure SDK for C Security Feature Bypass Vulnerability	7.4	More Details
CVE-2020-16971	Azure SDK for Java Security Feature Bypass Vulnerability	7.4	More Details
CVE-2020-5665	Improper check or handling of exceptional conditions in MELSEC iQ-F series FX5U(C) CPU unit firmware version 1.060 and earlier allows an attacker to cause a denial-of-service (DoS) condition on program execution and communication by sending a specially crafted ARP packet.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7788	This affects the package ini before 1.3.6. If an attacker submits a malicious INI file to an application that parses it with ini.parse, they will pollute the prototype on the application. This can be exploited further depending on the context.	7.3	More Details
CVE-2020-28456	The package s-cart/core before 4.4 are vulnerable to Cross-site Scripting (XSS) via the admin panel.	7.3	More Details
CVE-2020-28396	A vulnerability has been identified in SICAM A8000 CP-8000 (All versions < V16), SICAM A8000 CP-8021 (All versions < V16), SICAM A8000 CP-8022 (All versions < V16). A web server misconfiguration of the affected device can cause insecure ciphers usage by a user´s browser. An attacker in a privileged position could decrypt the communication and compromise confidentiality and integrity of the transmitted information.	7.3	More Details
CVE-2020-35382	SQL Injection in Classbooking before 2.4.1 via the username field of a CSV file when adding a new user.	7.2	More Details
CVE-2020-28457	This affects the package s-cart/core before 4.4. The search functionality of the admin dashboard in core/src/Admin/Controllers/AdminOrderController.phpindex is vulnerable to XSS.	7.2	More Details
CVE-2020-12594	A privilege escalation flaw allows a malicious, authenticated, privileged CLI user to escalate their privileges on the system and gain full control over the SMG appliance. This affects SMG prior to 10.7.4.	7.2	More Details
CVE-2020-23520	imcat 5.2 allows an authenticated file upload and consequently remote code execution via the picture functionality.	7.2	More Details
CVE-2020-24637	Two vulnerabilities in ArubaOS GRUB2 implementation allows for an attacker to bypass secureboot. Successful exploitation of this vulnerability this could lead to remote compromise of system integrity by allowing an attacker to load an untrusted or modified kernel in Aruba 9000 Gateway; Aruba 7000 Series Mobility Controllers; Aruba 7200 Series Mobility Controllers version(s): 2.1.0.1, 2.2.0.0 and below; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below ; 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below.	7.2	More Details
CVE-2019-19286	A vulnerability has been identified in XHQ (All Versions < 6.1). The web interface could allow SQL injection attacks if an attacker is able to modify content of particular web pages.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28072	A Remote Code Execution vulnerability exists in DourceCodester Alumni Management System 1.0. An authenticated attacker can upload arbitrary file in the gallery.php page and executing it on the server reaching the RCE.	7.2	More Details
CVE-2020-16102	Improper Authentication vulnerability in Gallagher Command Centre Server allows an unauthenticated remote attacker to create items with invalid configuration, potentially causing the server to crash and fail to restart. This issue affects: Gallagher Command Centre 8.30 versions prior to 8.30.1299(MR2); 8.20 versions prior to 8.20.1218(MR4); 8.10 versions prior to 8.10.1253(MR6); 8.00 versions prior to 8.00.1252(MR7); version 7.90 and prior versions.	7.1	More Details
CVE-2020-7776	This affects the package phpoffice/phpspreadsheet from 0.0.0. The library is vulnerable to XSS when creating an html output from an excel file by adding a comment on any cell. The root cause of this issue is within the HTML writer where user comments are concatenated as part of link and this is returned as HTML. A fix for this issue is available on commit 0ed5b800be2136bcb8fa9c1bdf59abc957a98845/master branch.	7.1	More Details
CVE-2020-17089	Microsoft SharePoint Elevation of Privilege Vulnerability	7.1	More Details
CVE-2020-14368	A flaw was found in Eclipse Che in versions prior to 7.14.0 that impacts CodeReady Workspaces. When configured with cookies authentication, Theia IDE doesn't properly set the SameSite value, allowing a Cross-Site Request Forgery (CSRF) and consequently allowing a cross-site WebSocket hijack on Theia IDE. This flaw allows an attacker to gain full access to the victim's workspace through the /services endpoint. To perform a successful attack, the attacker conducts a Man-in-the-middle attack (MITM) and tricks the victim into executing a request via an untrusted link, which performs the CSRF and the Socket hijack. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.1	More Details
CVE-2020-0474	In HalCamera::requestNewFrame of HalCamera.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169282240	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24447	Adobe Lightroom Classic version 10.0 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-24440	Adobe Prelude version 9.0.1 (and earlier) is affected by an uncontrolled search path element that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.0	More Details
CVE-2020-17103	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2020-26964	If the Remote Debugging via USB feature was enabled in Firefox for Android on an Android version prior to Android 6.0, untrusted apps could have connected to the feature and operated with the privileges of the browser to read and interact with web content. The feature was implemented as a unix domain socket, protected by the Android SELinux policy; however, SELinux was not enforced for versions prior to 6.0. This was fixed by removing the Remote Debugging via USB feature from affected devices. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83.	6.8	More Details
CVE-2020-17099	Windows Lock Screen Security Feature Bypass Vulnerability	6.8	More Details
CVE-2020-5636	Aterm SA3500G firmware versions prior to Ver. 3.5.9 allows an attacker with an administrative privilege to send a specially crafted request to a specific URL, which may result in an arbitrary command execution.	6.8	More Details
CVE-2020-5637	Improper validation of integrity check value vulnerability in Aterm SA3500G firmware versions prior to Ver. 3.5.9 allows an attacker with an administrative privilege to execute a malicious program.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12148	A command injection flaw identified in the nslookup API in Silver Peak Unity ECOSTM (ECOS) appliance software could allow an attacker to execute arbitrary commands with the privileges of the web server running on the EdgeConnect appliance. An attacker could exploit this vulnerability to establish an interactive channel, effectively taking control of the target system. This vulnerability can be exploited by an attacker with authenticated access to the Orchestrator UI or EdgeConnect UI. This affects all ECOS versions prior to : 8.1.9.15, 8.3.0.8, 8.3.1.2, 8.3.2.0, 9.0.2.0, and 9.1.0.0.	6.8	More Details
CVE-2020-12149	The configuration backup/restore function in Silver Peak Unity ECOSTM (ECOS) appliance software was found to directly incorporate the user-controlled config filename in a subsequent shell command, allowing an attacker to manipulate the resulting command by injecting valid OS command input. This vulnerability can be exploited by an attacker with authenticated access to the Orchestrator UI or EdgeConnect UI. This affects all ECOS versions prior to: 8.1.9.15, 8.3.0.8, 8.3.1.2, 8.3.2.0, 9.0.2.0, and 9.1.0.0.	6.8	More Details
CVE-2020-0465	In various methods of hid-multitouch.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-162844689References: Upstream kernel	6.8	More Details
CVE-2020-28220	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in Modicon M258 Firmware (All versions prior to V5.0.4.11) and SoMachine/SoMachine Motion software (All versions), that could cause a buffer overflow when the length of a file transferred to the webserver is not verified.	6.8	More Details
CVE-2020-15375	Brocade Fabric OS versions before v9.0.0, v8.2.2c, v8.2.1e, v8.1.2k, v8.2.0_CBN3, v7.4.2g contain an improper input validation weakness in the command line interface when seccrypptocfg is invoked. The vulnerability could allow a local authenticated user to run arbitrary commands and perform escalation of privileges.	6.7	More Details
CVE-2020-27066	In xfrm6_tunnel_free_spi of net/ipv6/xfrm6_tunnel.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168043318	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0484	In destroyResources of ComposerClient.h, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155769496	6.7	More Details
CVE-2020-0483	In DrmManagerService::~DrmManagerService() of DrmManagerService.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155647761	6.7	More Details
CVE-2020-27036	In phNxpNciHal_send_ext_cmd of phNxpNciHal_ext.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153731369	6.7	More Details
CVE-2020-27777	A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (usually due to Secure Boot) guest system running on top of PowerVM or KVM hypervisors (pseries platform) a root like local user could use this flaw to further increase their privileges to that of a running kernel.	6.7	More Details
CVE-2020-17117	Microsoft Exchange Remote Code Execution Vulnerability	6.6	More Details
CVE-2019-19287	A vulnerability has been identified in XHQ (All Versions < 6.1). The web interface could allow attackers to traverse through the file system of the server based by sending specially crafted packets over the network without authentication.	6.5	More Details
CVE-2020-17133	Microsoft Dynamics Business Central/NAV Information Disclosure	6.5	More Details
CVE-2020-16996	Kerberos Security Feature Bypass Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0491	In readBlock of MatroskaExtractor.cpp, there is a possible denial of service due to resource exhaustion. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156819528	6.5	More Details
CVE-2020-17130	Microsoft Excel Security Feature Bypass Vulnerability	6.5	More Details
CVE-2020-26955	When a user downloaded a file in Firefox for Android, if a cookie is set, it would have been re-sent during a subsequent file download operation on the same domain, regardless of whether the original and subsequent request were in private and non-private browsing modes. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83.	6.5	More Details
CVE-2020-0490	In floor1_info_unpack of floor1.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155560008	6.5	More Details
CVE-2020-17119	Microsoft Outlook Information Disclosure Vulnerability	6.5	More Details
CVE-2020-15733	An Origin Validation Error vulnerability in the SafePay component of Bitdefender Antivirus Plus allows a web resource to misrepresent itself in the URL bar. This issue affects: Bitdefender Antivirus Plus versions prior to 25.0.7.29.	6.5	More Details
CVE-2020-0488	In ihevc_inter_pred_chroma_copy_ssse3 of ihevc_inter_pred_filters_ssse3_intr.c, there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-158484516	6.5	More Details
CVE-2020-26957	OneCRL was non-functional in the new Firefox for Android due to a missing service initialization. This could result in a failure to enforce some certificate revocations. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26826	Process Integration Monitoring of SAP NetWeaver AS JAVA, versions - 7.31, 7.40, 7.50, allows an attacker to upload any file (including script files) without proper file format validation, leading to Unrestricted File Upload.	6.5	More Details
CVE-2020-7337	Incorrect Permission Assignment for Critical Resource vulnerability in McAfee VirusScan Enterprise (VSE) prior to 8.8 Patch 16 allows local administrators to bypass local security protection through VSE not correctly integrating with Windows Defender Application Control via careful manipulation of the Code Integrity checks.	6.5	More Details
CVE-2020-0492	In BitstreamFillCache of bitstream.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154058264	6.5	More Details
CVE-2020-27147	The REST API component of TIBCO Software Inc.'s TIBCO PartnerExpress contains a vulnerability that theoretically allows an unauthenticated attacker with network access to obtain an authenticated login URL for the affected system via a REST API. Affected releases are TIBCO Software Inc.'s TIBCO PartnerExpress: version 6.2.0.	6.5	More Details
CVE-2020-0494	In ih264d_parse_ave of ih264d_sei.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-152895390	6.5	More Details
CVE-2020-26257	Matrix is an ecosystem for open federated Instant Messaging and VoIP. Synapse is a reference "homeserver" implementation of Matrix. A malicious or poorly-implemented homeserver can inject malformed events into a room by specifying a different room id in the path of a `/send_join`, `/send_leave`, `/invite` or `/exchange_third_party_invite` request. This can lead to a denial of service in which future events will not be correctly sent to other servers over federation. This affects any server which accepts federation requests from untrusted servers. The Matrix Synapse reference implementation before version 1.23.1 the implementation is vulnerable to this injection attack. Issue is fixed in version 1.23.1. As a workaround homeserver administrators could limit access to the federation API to trusted servers (for example via `federation_domain_whitelist`).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26965	Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the software keyboard to remember the typed password. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	6.5	More Details
CVE-2020-26966	Searching for a single word from the address bar caused an mDNS request to be sent on the local network searching for a hostname consisting of that string; resulting in an information leak. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	6.5	More Details
CVE-2020-26264	Go Ethereum, or "Geth", is the official Golang implementation of the Ethereum protocol. In Geth before version 1.9.25 a denial-of-service vulnerability can make a LES server crash via malicious GetProofsV2 request from a connected LES client. This vulnerability only concerns users explicitly enabling les server; disabling les prevents the exploit. The vulnerability was patched in version 1.9.25.	6.5	More Details
CVE-2020-26967	When listening for page changes with a Mutation Observer, a malicious web page could confuse Firefox Screenshots into interacting with elements other than those that it injected into the page. This would lead to internal errors and unexpected behavior in the Screenshots code. This vulnerability affects Firefox < 83.	6.5	More Details
CVE-2019-4738	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 and 6.0.0.0 through 6.0.3.1 discloses sensitive information to an authenticated user from the dashboard UI which could be used in further attacks against the system. IBM X-Force ID: 172753.	6.5	More Details
CVE-2020-28218	A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists in Easergy T300 (firmware 2.7 and older), that would allow an attacker to trick a user into initiating an unintended action.	6.5	More Details
CVE-2020-17511	In Airflow versions prior to 1.10.13, when creating a user using airflow CLI, the password gets logged in plain text in the Log table in Airflow Metadatase. Same happened when creating a Connection with a password field.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29483	An issue was discovered in Xen through 4.14.x. Xenstored and guests communicate via a shared memory page using a specific protocol. When a guest violates this protocol, xenstored will drop the connection to that guest. Unfortunately, this is done by just removing the guest from xenstored's internal management, resulting in the same actions as if the guest had been destroyed, including sending an @releaseDomain event. @releaseDomain events do not say that the guest has been removed. All watchers of this event must look at the states of all guests to find the guest that has been removed. When an @releaseDomain is generated due to a domain xenstored protocol violation, because the guest is still running, the watchers will not react. Later, when the guest is actually destroyed, xenstored will no longer have it stored in its internal data base, so no further @releaseDomain event will be sent. This can lead to a zombie domain; memory mappings of that guest's memory will not be removed, due to the missing event. This zombie domain will be cleaned up only after another domain is destroyed, as that will trigger another @releaseDomain event. If the device model of the guest that violated the Xenstore protocol is running in a stub-domain, a use-after-free case could happen in xenstored, after having removed the guest from its internal data base, possibly resulting in a crash of xenstored. A malicious guest can block resources of the host for a period after its own death. Guests with a stub domain device model can eventually crash xenstored, resulting in a more serious denial of service (the prevention of any further domain management operations). Only the C variant of Xenstore is affected; the Ocaml variant is not affected. Only HVM guests with a stubdom device model can cause a serious DoS.	6.5	More Details
CVE-2020-29568	An issue was discovered in Xen through 4.14.x. Some OSes (such as Linux, FreeBSD, and NetBSD) are processing watch events using a single thread. If the events are received faster than the thread is able to handle, they will get queued. As the queue is unbounded, a guest may be able to trigger an OOM in the backend. All systems with a FreeBSD, Linux, or NetBSD (any version) dom0 are vulnerable.	6.5	More Details
CVE-2020-26961	When DNS over HTTPS is in use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these addresses were erroneously let through, leading to a potential DNS Rebinding attack. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	6.5	More Details
CVE-2020-25838	Unauthorized disclosure of sensitive information vulnerability in Micro Focus Filr product. Affecting all 3.x and 4.x versions. The vulnerability could be exploited to disclose unauthorized sensitive information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27038	In process of C2SoftVorbisDec.cpp, there is a possible resource exhaustion due to a memory leak. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154302257	6.5	More Details
CVE-2020-27029	In TextView of TextView.java, there is a possible app hang due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-140218875	6.5	More Details
CVE-2020-17135	Azure DevOps Server Spoofing Vulnerability	6.4	More Details
CVE-2020-26260	BookStack is a platform for storing and organising information and documentation. In BookStack before version 0.30.5, a user with permissions to edit a page could set certain image URL's to manipulate functionality in the exporting system, which would allow them to make server side requests and/or have access to a wider scope of files within the BookStack file storage locations. The issue was addressed in BookStack v0.30.5. As a workaround, page edit permissions could be limited to only those that are trusted until you can upgrade.	6.4	More Details
CVE-2020-27067	In the l2tp subsystem, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-152409173	6.4	More Details
CVE-2020-26828	SAP Disclosure Management, version - 10.1, provides capabilities for authorized users to upload and download content of specific file type. In some file types it is possible to enter formulas which can call external applications or execute scripts. The execution of a payload (script) on target machine could be used to steal and modify the data available in the spreadsheet	6.4	More Details
CVE-2020-7339	Use of a Broken or Risky Cryptographic Algorithm vulnerability in McAfee Database Security Server and Sensor prior to 4.8.0 in the form of a SHA1 signed certificate that would allow an attacker on the same local network to potentially intercept communication between the Server and Sensors.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29567	An issue was discovered in Xen 4.14.x. When moving IRQs between CPUs to distribute the load of IRQ handling, IRQ vectors are dynamically allocated and de-allocated on the relevant CPUs. De-allocation has to happen when certain constraints are met. If these conditions are not met when first checked, the checking CPU may send an interrupt to itself, in the expectation that this IRQ will be delivered only after the condition preventing the cleanup has cleared. For two specific IRQ vectors, this expectation was violated, resulting in a continuous stream of self-interrupts, which renders the CPU effectively unusable. A domain with a passed through PCI device can cause lockup of a physical CPU, resulting in a Denial of Service (DoS) to the entire host. Only x86 systems are vulnerable. Arm systems are not vulnerable. Only guests with physical PCI devices passed through to them can exploit the vulnerability.	6.2	More Details
CVE-2020-29571	An issue was discovered in Xen through 4.14.x. A bounds check common to most operation time functions specific to FIFO event channels depends on the CPU observing consistent state. While the producer side uses appropriately ordered writes, the consumer side isn't protected against re-ordered reads, and may hence end up de-referencing a NULL pointer. Malicious or buggy guest kernels can mount a Denial of Service (DoS) attack affecting the entire system. Only Arm systems may be vulnerable. Whether a system is vulnerable depends on the specific CPU. x86 systems are not vulnerable.	6.2	More Details
CVE-2020-29570	An issue was discovered in Xen through 4.14.x. Recording of the per-vCPU control block mapping maintained by Xen and that of pointers into the control block is reversed. The consumer assumes, seeing the former initialized, that the latter are also ready for use. Malicious or buggy guest kernels can mount a Denial of Service (DoS) attack affecting the entire system.	6.2	More Details
CVE-2020-29304	A cross-site scripting (XSS) vulnerability exists in the SabaiApps WordPress Directories Pro plugin version 1.3.45 and previous, allows attackers who have convinced a site administrator to import a specially crafted CSV file to inject arbitrary web script or HTML as the victim is proceeding through the file import workflow.	6.1	More Details
CVE-2020-28857	OpenAsset Digital Asset Management (DAM) through 12.0.19, does not correctly sanitize user supplied input in multiple parameters and endpoints, allowing for stored cross-site scripting attacks.	6.1	More Details
CVE-2020-25627	The moodlenetprofile user profile field required extra sanitizing to prevent a stored XSS risk. This affects versions 3.9 to 3.9.1. Fixed in 3.9.2.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4849	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.19 Interim Fix 7 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a vitcim to a phishing site. IBM X-Force ID: 190294.	6.1	More Details
CVE-2020-29257	Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the q parameter to feedback.php.	6.1	More Details
CVE-2020-29258	Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the w parameter to index.php.	6.1	More Details
CVE-2020-35416	Multiple cross-site scripting (XSS) vulnerabilities exist in PHPJabbers Appointment Scheduler 2.3, in the index.php admin login webpage (with different request parameters), allows remote attackers to inject arbitrary web script or HTML.	6.1	More Details
CVE-2019-19288	A vulnerability has been identified in XHQ (All Versions < 6.1). The web interface could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.	6.1	More Details
CVE-2020-26951	A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after sanitization. An attacker already capable of exploiting an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	6.1	More Details
CVE-2020-28859	OpenAsset Digital Asset Management (DAM) through 12.0.19 does not correctly sanitize user supplied input in multiple parameters and endpoints, allowing for reflected cross-site scripting attacks.	6.1	More Details
CVE-2020-23957	Pega Platform through 8.4.x is affected by Cross Site Scripting (XSS) via the ConnectionID parameter, as demonstrated by a pyActivity=Data-TRACERSettings.pzStartTracerSession request to a PRAuth URI.	6.1	More Details
CVE-2020-26836	SAP Solution Manager (Trace Analysis), version - 720, allows for misuse of a parameter in the application URL leading to Open Redirect vulnerability, an attacker can enter a link to malicious site which could trick the user to enter credentials or download malicious software, as a parameter in the application URL and share it with the end user who could potentially become a victim of the attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26956	In some cases, removing HTML elements during sanitization would keep existing SVG event handlers and therefore lead to XSS. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	6.1	More Details
CVE-2020-29303	A cross-site scripting (XSS) vulnerability in the SabaiApp Directories Pro plugin 1.3.45 for WordPress allows remote attackers to inject arbitrary web script or HTML via a POST to /wp-admin/admin.php?page=drts/directories&q=%2F with _drts_form_build_id parameter containing the XSS payload and _t_ parameter set to an invalid or non-existent CSRF token.	6.1	More Details
CVE-2020-26958	Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	6.1	More Details
CVE-2020-26835	SAP NetWeaver AS ABAP, versions - 740, 750, 751, 752, 753, 754 , does not sufficiently encode URL which allows an attacker to input malicious java script in the URL which could be executed in the browser resulting in Reflected Cross-Site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2020-2491	This cross-site scripting vulnerability in Photo Station allows remote attackers to inject malicious code. QANP We have already fixed this vulnerability in the following versions of Photo Station. QTS 4.5.1: Photo Station 6.0.12 and later QTS 4.4.3: Photo Station 6.0.12 and later QTS 4.3.6: Photo Station 5.7.12 and later QTS 4.3.4: Photo Station 5.7.13 and later QTS 4.3.3: Photo Station 5.4.10 and later QTS 4.2.6: Photo Station 5.2.11 and later	6.1	More Details
CVE-2020-26962	Cross-origin iframes that contained a login form could have been recognized by the login autofill service, and populated. This could have been used in clickjacking attacks, as well as be read across partitions in dynamic first party isolation. This vulnerability affects Firefox < 83.	6.1	More Details
CVE-2020-17515	The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions prior to 1.10.13. This is same as CVE-2020-13944 but the implemented fix in Airflow 1.10.13 did not fix the issue completely.	6.1	More Details
CVE-2020-29455	A cross-Site Scripting (XSS) vulnerability in this.showInvalid and this.showInvalidCountry in SmartyStreets liveAddressPlugin.js 3.2 allows remote attackers to inject arbitrary web script or HTML via any address parameter (e.g., street or country).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35396	EGavilan Barcodes generator 1.0 is affected by: Cross Site Scripting (XSS) via the index.php. An Attacker is able to inject the XSS payload in the web application each time a user visits the website.	6.1	More Details
CVE-2020-35395	XSS in the Add Expense Component of EGavilan Media Expense Management System 1.0 allows an attacker to permanently store malicious JavaScript code via the 'description' field	6.1	More Details
CVE-2020-2498	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in certificate configuration. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later	6.1	More Details
CVE-2020-2497	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in System Connection Logs. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later	6.1	More Details
CVE-2020-2496	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in File Station. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later	6.1	More Details
CVE-2020-2495	If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in File Station. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2494	This cross-site scripting vulnerability in Music Station allows remote attackers to inject malicious code. QANP have already fixed this vulnerability in the following versions of Music Station. QuTS hero h4.5.1: Music Station 5.3.13 and later QTS 4.5.1: Music Station 5.3.12 and later QTS 4.4.3: Music Station 5.3.12 and later	6.1	More Details
CVE-2020-2493	This cross-site scripting vulnerability in Multimedia Console allows remote attackers to inject malicious code. QANP have already fixed this vulnerability in Multimedia Console 1.1.5 and later.	6.1	More Details
CVE-2020-35200	Ignite Realtime Openfire 4.6.0 has plugins/clientcontrol/spark-form.jsp Reflective XSS.	6.1	More Details
CVE-2020-29484	An issue was discovered in Xen through 4.14.x. When a Xenstore watch fires, the xenstore client that registered the watch will receive a Xenstore message containing the path of the modified Xenstore entry that triggered the watch, and the tag that was specified when registering the watch. Any communication with xenstored is done via Xenstore messages, consisting of a message header and the payload. The payload length is limited to 4096 bytes. Any request to xenstored resulting in a response with a payload longer than 4096 bytes will result in an error. When registering a watch, the payload length limit applies to the combined length of the watched path and the specified tag. Because watches for a specific path are also triggered for all nodes below that path, the payload of a watch event message can be longer than the payload needed to register the watch. A malicious guest that registers a watch using a very large tag (i.e., with a registration operation payload length close to the 4096 byte limit) can cause the generation of watch events with a payload length larger than 4096 bytes, by writing to Xenstore entries below the watched path. This will result in an error condition in xenstored. This error can result in a NULL pointer dereference, leading to a crash of xenstored. A malicious guest administrator can cause xenstored to crash, leading to a denial of service. Following a xenstored crash, domains may continue to run, but management operations will be impossible. Only C xenstored is affected, oxenstored is not affected.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29486	An issue was discovered in Xen through 4.14.x. Nodes in xenstore have an ownership. In oxenstored, a owner could give a node away. However, node ownership has quota implications. Any guest can run another guest out of quota, or create an unbounded number of nodes owned by dom0, thus running xenstored out of memory A malicious guest administrator can cause a denial of service against a specific guest or against the whole host. All systems using oxenstored are vulnerable. Building and using oxenstored is the default in the upstream Xen distribution, if the Ocaml compiler is available. Systems using C xenstored are not vulnerable.	6.0	More Details
CVE-2020-29482	An issue was discovered in Xen through 4.14.x. A guest may access xenstore paths via absolute paths containing a full pathname, or via a relative path, which implicitly includes /local/domain/$DOMID for their own domain id. Management tools must access paths in guests' namespaces, necessarily using absolute paths. oxenstored imposes a pathname limit that is applied solely to the relative or absolute path specified by the client. Therefore, a guest can create paths in its own namespace which are too long for management tools to access. Depending on the toolstack in use, a malicious guest administrator might cause some management tools and debugging operations to fail. For example, a guest administrator can cause "xenstore-ls -r" to fail. However, a guest administrator cannot prevent the host administrator from tearing down the domain. All systems using oxenstored are vulnerable. Building and using oxenstored is the default in the upstream Xen distribution, if the Ocaml compiler is available. Systems using C xenstored are not vulnerable.	6.0	More Details
CVE-2020-15023	Askey AP5100W devices through AP5100W_Dual_SIG_1.01.097 are affected by WPS PIN offline brute-force cracking. This arises because of issues with the random number selection for the Diffie-Hellman exchange. By capturing an attempted (and even failed) WPS authentication attempt, it is possible to brute force the overall authentication exchange. This allows an attacker to obtain the recovered WPS PIN in minutes or even seconds, and eventually obtain the Wi-Fi PSK key, gaining access to the Wi=Fi network.	5.9	More Details
CVE-2020-24444	AEM Forms SP6 add-on for AEM 6.5.6.0 and Forms add-on package for AEM 6.4 Service Pack 8 Cumulative Fix Pack 2 (6.4.8.2) have a blind Server-Side Request Forgery (SSRF) vulnerability. This vulnerability could be exploited by an unauthenticated attacker to gather information about internal systems that reside on the same network.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27350	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1;	5.7	More Details
CVE-2020-10146	The Microsoft Teams online service contains a stored cross-site scripting vulnerability in the displayName parameter that can be exploited on Teams clients to obtain sensitive information such as authentication tokens and to possibly execute arbitrary commands. This vulnerability was fixed for all Teams users in the online service on or around October 2020.	5.7	More Details
CVE-2020-35207	An issue was discovered in the LogMein LastPass Password Manager (aka com.lastpass.ilastpass) app 4.8.11.2403 for iOS. The PIN authentication for unlocking can be bypassed by forcing the authentication result to be true through runtime manipulation. In other words, an attacker could authenticate with an arbitrary PIN. NOTE: the vendor has indicated that this is not an attack of interest within the context of their threat model, which excludes jailbroken devices	5.7	More Details
CVE-2020-35208	An issue was discovered in the LogMein LastPass Password Manager (aka com.lastpass.ilastpass) app 4.8.11.2403 for iOS. The password authentication for unlocking can be bypassed by forcing the authentication result to be true through runtime manipulation. In other words, an attacker could authenticate with an arbitrary password. NOTE: the vendor has indicated that this is not an attack of interest within the context of their threat model, which excludes jailbroken devices	5.7	More Details
CVE-2020-27825	A use-after-free flaw was found in kernel/trace/ring_buffer.c in Linux kernel (before 5.10-rc1). There was a race problem in trace_open and resize of cpu buffer running parallely on different cpus, may cause a denial of service problem (DOS). This flaw could even allow a local attacker with special user privilege to a kernel information leak threat.	5.7	More Details
CVE-2020-7789	This affects the package node-notifier before 9.0.0. It allows an attacker to run arbitrary commands on Linux machines due to the options params not being sanitised when being passed an array.	5.6	More Details
CVE-2020-27027	In nfc_ncif_proc_get_routing of nfc_ncif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-122358602	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0495	In decode_Huffman of JBig2_SddProc.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155473137	5.5	More Details
CVE-2020-28203	An issue was discovered in Foxit Reader and PhantomPDF 10.1.0.37527 and earlier. There is a null pointer access/dereference while opening a crafted PDF file, leading the application to crash (denial of service).	5.5	More Details
CVE-2020-27047	In ce_t4t_update_binary of ce_t4t.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157649298	5.5	More Details
CVE-2020-29566	An issue was discovered in Xen through 4.14.x. When they require assistance from the device model, x86 HVM guests must be temporarily de-scheduled. The device model will signal Xen when it has completed its operation, via an event channel, so that the relevant vCPU is rescheduled. If the device model were to signal Xen without having actually completed the operation, the de-schedule / re-schedule cycle would repeat. If, in addition, Xen is resignalled very quickly, the re-schedule may occur before the de-schedule was fully complete, triggering a shortcut. This potentially repeating process uses ordinary recursive function calls, and thus could result in a stack overflow. A malicious or buggy stubdomain serving a HVM guest can cause Xen to crash, resulting in a Denial of Service (DoS) to the entire host. Only x86 systems are affected. Arm systems are not affected. Only x86 stubdomains serving HVM guests can exploit the vulnerability.	5.5	More Details
CVE-2020-27349	Aptdaemon performed policykit checks after interacting with potentially untrusted files with elevated privileges. This affected versions prior to 1.1.1+bzr982-0ubuntu34.1, 1.1.1+bzr982-0ubuntu32.3, 1.1.1+bzr982-0ubuntu19.5, 1.1.1+bzr982-0ubuntu14.5.	5.5	More Details
CVE-2020-2020	An improper handling of exceptional conditions vulnerability in Cortex XDR Agent allows a local authenticated Windows user to create files in the software's internal program directory that prevents the Cortex XDR Agent from starting. The exceptional condition is persistent and prevents Cortex XDR Agent from starting when the software or machine is restarted. This issue impacts: Cortex XDR Agent 5.0 versions earlier than 5.0.10; Cortex XDR Agent 6.1 versions earlier than 6.1.7; Cortex XDR Agent 7.0 versions earlier than 7.0.3; Cortex XDR Agent 7.1 versions earlier than 7.1.2.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0019	In the Broadcom Nexus firmware, there is an insecure default password. This could lead to local information disclosure in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-171413798	5.5	More Details
CVE-2020-0470	In extend_frame_highbd of restoration.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-166268541	5.5	More Details
CVE-2020-0469	In addEscrowToken of LockSettingsService.java, there is a possible loss of the synthetic password due to logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168692734	5.5	More Details
CVE-2020-0468	In listen() and related functions of TelephonyRegistry.java, there is a possible permissions bypass of location permissions due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-158484422	5.5	More Details
CVE-2020-0244	In writeBurstBufferBytes of SPDIFEncoder.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no clear exfiltration path, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145262423	5.5	More Details
CVE-2020-27039	In postNotification of ServiceRecord.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153878498	5.5	More Details
CVE-2020-0280	In nci_proc_ee_management_rsp of nci_hrcv.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-136565424	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27041	In showProvisioningNotification of ConnectivityService.java, there is an unsafe PendingIntent. This could lead to local information disclosure of notification data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154928507	5.5	More Details
CVE-2020-0496	In CPDF_RenderStatus::LoadSMask of cpdf_renderstatus.cpp, there is a possible memory corruption due to a use-after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-149481220	5.5	More Details
CVE-2020-0497	In canUseBiometric of BiometricServiceBase, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-158481661	5.5	More Details
CVE-2020-29485	An issue was discovered in Xen 4.6 through 4.14.x. When acting upon a guest XS_RESET_WATCHES request, not all tracking information is freed. A guest can cause unbounded memory usage in oxenstored. This can lead to a system-wide DoS. Only systems using the Ocaml Xenstored implementation are vulnerable. Systems using the C Xenstored implementation are not vulnerable.	5.5	More Details
CVE-2020-27035	In priorLinearAllocation of C2AllocatorIon.cpp, there is a possible use-after-free due to improper locking. This could lead to local information disclosure in the media codec with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-152239213	5.5	More Details
CVE-2020-0498	In decode_packed_entry_number of codebook.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160633884	5.5	More Details
CVE-2020-0493	In CPDF_SampledFunc::v_Call of cpdf_sampledfunc.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150615407	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0500	In startInputUncheckedLocked of InputMethodManager.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154913391	5.5	More Details
CVE-2020-27025	In EapFailureNotifier.java and SimRequiredNotifier.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156008365	5.5	More Details
CVE-2020-27026	During boot, the device unlock interface behaves differently depending on if a fingerprint registered to the device is present. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-79776455	5.5	More Details
CVE-2020-27034	In createSimSelectNotification of SimSelectNotification.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153556754	5.5	More Details
CVE-2020-0467	In onUserStopped of Vpn.java, there is a possible resetting of user preferences due to a logic issue. This could lead to local information disclosure of secure network traffic over a non-VPN link with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-168500792	5.5	More Details
CVE-2020-27032	In getRadioAccessFamily of PhoneInterfaceManager.java, there is a possible read of privileged data due to a missing permission check. This could lead to local information disclosure of radio data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150857259	5.5	More Details
CVE-2020-0477	In sendLinkConfigurationChangedBroadcast of ClientModeImpl.java, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of the current network configuration with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162246414	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16590	A double free vulnerability exists in the Binary File Descriptor (BFD) (aka libbrd) in GNU Binutils 2.35 in the process_symbol_table, as demonstrated in readelf, via a crafted file.	5.5	More Details
CVE-2020-16587	A heap-based buffer overflow vulnerability exists in Academy Software Foundation OpenEXR 2.3.0 in chunkOffsetReconstruction in ImfMultiPartInputFile.cpp that can cause a denial of service via a crafted EXR file.	5.5	More Details
CVE-2020-28214	A CWE-760: Use of a One-Way Hash with a Predictable Salt vulnerability exists in Modicon M221 (all references, all versions), that could allow an attacker to pre-compute the hash value using dictionary attack technique such as rainbow tables, effectively disabling the protection that an unpredictable salt would provide.	5.5	More Details
CVE-2020-26407	A XSS vulnerability exists in Gitlab CE/EE from 12.4 before 13.4.7, 13.5 before 13.5.5, and 13.6 before 13.6.2 that allows an attacker to perform cross-site scripting to other users via importing a malicious project	5.5	More Details
CVE-2020-25231	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3), LOGO! Soft Comfort (All versions < V8.3). The encryption of program data for the affected devices uses a static key. An attacker could use this key to extract confidential information from protected program files.	5.5	More Details
CVE-2020-25233	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). The firmware update of affected devices contains the private RSA key that is used as a basis for encryption of communication with the device.	5.5	More Details
CVE-2020-0464	In resolv_cache_lookup of res_cache.cpp, there is a possible side channel information disclosure. This could lead to local information disclosure of accessed web resources with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150371903	5.5	More Details
CVE-2020-17126	Microsoft Excel Information Disclosure Vulnerability	5.5	More Details
CVE-2020-16599	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.35, in _bfd_elf_get_symbol_version_string, as demonstrated in nm-new, that can cause a denial of service via a crafted file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17098	Windows GDI+ Information Disclosure Vulnerability	5.5	More Details
CVE-2020-17094	Windows Error Reporting Information Disclosure Vulnerability	5.5	More Details
CVE-2020-16593	A Null Pointer Dereference vulnerability exists in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.35, in scan_unit_for_symbols, as demonstrated in addr2line, that can cause a denial of service via a crafted file.	5.5	More Details
CVE-2020-17138	Windows Error Reporting Information Disclosure Vulnerability	5.5	More Details
CVE-2020-16588	A Null Pointer Deference issue exists in Academy Software Foundation OpenEXR 2.3.0 in generatePreview in makePreview.cpp that can cause a denial of service via a crafted EXR file.	5.5	More Details
CVE-2020-16589	A head-based buffer overflow exists in Academy Software Foundation OpenEXR 2.3.0 in writeTileData in ImfTiledOutputFile.cpp that can cause a denial of service via a crafted EXR file.	5.5	More Details
CVE-2020-16591	A Denial of Service vulnerability exists in the Binary File Descriptor (BFD) in GNU Binutils 2.35 due to an invalid read in process_symbol_table, as demonstrated in readeif.	5.5	More Details
CVE-2020-16592	A use after free issue exists in the Binary File Descriptor (BFD) library (aka libbfd) in GNU Binutils 2.34 in bfd_hash_lookup, as demonstrated in nm-new, that can cause a denial of service via a crafted file.	5.5	More Details
CVE-2018-16243	SolarWinds Database Performance Analyzer (DPA) 11.1.468 and 12.0.3074 have several persistent XSS vulnerabilities, related to logViewer.iwc, centralManage.cen, userAdministration.iwc, database.iwc, alertManagement.iwc, eventAnnotations.iwc, and central.cen.	5.4	More Details
CVE-2020-29259	Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the subject or feedback parameter to feedback.php.	5.4	More Details
CVE-2020-26834	SAP HANA Database, version - 2.0, does not correctly validate the username when performing SAML bearer token-based user authentication. It is possible to manipulate a valid existing SAML bearer token to authenticate as a user whose name is identical to the truncated username for whom the SAML bearer token was issued.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35199	Ignite Realtime Openfire 4.6.0 has create-bookmark.jsp groupchatJID Stored XSS.	5.4	More Details
CVE-2020-35201	Ignite Realtime Openfire 4.6.0 has create-bookmark.jsp users Stored XSS.	5.4	More Details
CVE-2020-35132	An XSS issue has been discovered in phpLDAPadmin before 1.2.6.2 that allows users to store malicious values that may be executed by other users at a later time via get_request in lib/function.php.	5.4	More Details
CVE-2020-35127	Ignite Realtime Openfire 4.6.0 has plugins/bookmarks/create-bookmark.jsp Stored XSS.	5.4	More Details
CVE-2020-35202	Ignite Realtime Openfire 4.6.0 has plugins/dbaccess/db-access.jsp sql Stored XSS.	5.4	More Details
CVE-2019-19284	A vulnerability has been identified in XHQ (All Versions < 6.1). The web interface could allow Cross-Site Scripting (XSS) attacks if an attacker is able to modify content of particular web pages, causing the application to behave in unexpected ways for legitimate users.	5.4	More Details
CVE-2020-17145	Azure DevOps Server and Team Foundation Services Spoofing Vulnerability	5.4	More Details
CVE-2019-19285	A vulnerability has been identified in XHQ (All Versions < 6.1). The web interface could allow injections that could lead to XSS attacks if unsuspecting users are tricked into accessing a malicious link.	5.4	More Details
CVE-2020-35236	The GitLab Webhook Handler in amazee.io Lagoon before 1.12.3 has incorrect access control associated with project deletion.	5.3	More Details
CVE-2020-35176	In AWStats through 7.8, cgi-bin/awstats.pl?config= accepts a partial absolute pathname (omitting the initial /etc), even though it was intended to only read a file in the /etc/awstats/awstats.conf format. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000501 and CVE-2020-29600.	5.3	More Details
CVE-2020-5950	On BIG-IP 14.1.0-14.1.2.6, undisclosed endpoints in iControl REST allow for a reflected XSS attack, which could lead to a complete compromise of the BIG-IP system if the victim user is granted the admin role.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-35175	Frappe Framework 12 and 13 does not properly validate the HTTP method for the frappe.client API.	5.3	More Details
CVE-2020-17470	An issue was discovered in FNET through 4.6.4. The code that initializes the DNS client interface structure does not set sufficiently random transaction IDs (they are always set to 1 in _fnet_dns_poll in fnet_dns.c). This significantly simplifies DNS cache poisoning attacks.	5.3	More Details
CVE-2020-35149	lib/utils.js in mquery before 3.2.3 allows a pollution attack because a special property (e.g., __proto__) can be copied during a merge or clone operation.	5.3	More Details
CVE-2020-26265	Go Ethereum, or "Geth", is the official Golang implementation of the Ethereum protocol. In Geth from version 1.9.4 and before version 1.9.20 a consensus-vulnerability could cause a chain split, where vulnerable versions refuse to accept the canonical chain. The fix was included in the Paragade release version 1.9.20. No individual workaround patches have been made -- all users are recommended to upgrade to a newer version.	5.3	More Details
CVE-2020-7790	This affects the package spatie/browsershot from 0.0.0. By specifying a URL in the file:// protocol an attacker is able to include arbitrary files in the resultant PDF.	5.3	More Details
CVE-2020-26417	Information disclosure via GraphQL in GitLab CE/EE 13.1 and later exposes private group and project membership. This affects versions >=13.6 to <13.6.2, >=13.5 to <13.5.5, and >=13.1 to <13.4.7.	5.3	More Details
CVE-2020-26413	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4 before 13.6.2. Information disclosure via GraphQL results in user email being unexpectedly visible.	5.3	More Details
CVE-2020-10770	A flaw was found in Keycloak before 13.0.0, where it is possible to force the server to call out an unverified URL using the OIDC parameter request_uri. This flaw allows an attacker to use this parameter to execute a Server-side request forgery (SSRF) attack.	5.3	More Details
CVE-2020-26408	A limited information disclosure vulnerability exists in Gitlab CE/EE from >= 12.2 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2 that allows an attacker to view limited information in user's private profile	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7549	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP.	5.3	More Details
CVE-2020-7541	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules (see security notification for affected versions), that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP.	5.3	More Details
CVE-2020-17513	In Apache Airflow versions prior to 1.10.13, the Charts and Query View of the old (Flask-admin based) UI were vulnerable for SSRF attack.	5.3	More Details
CVE-2020-29666	In Lan ATMService M3 ATM Monitoring System 6.1.0, due to a directory-listing vulnerability, a remote attacker can view log files, located in /websocket/logs/, that contain a user's cookie values and the predefined developer's cookie value.	5.3	More Details
CVE-2020-17120	Microsoft SharePoint Information Disclosure Vulnerability	5.3	More Details
CVE-2020-8937	An arbitrary memory overwrite vulnerability in Asylo versions up to 0.6.0 allows an attacker to make a host call to enc_untrusted_create_wait_queue that uses a pointer queue that relies on UntrustedLocalMemcpy, which fails to validate where the pointer is located. This allows an attacker to write memory values from within the enclave. We recommend upgrading past commit a37fb6a0e7daf30134dbbf357c9a518a1026aa02	5.3	More Details
CVE-2020-28861	OpenAsset Digital Asset Management (DAM) 12.0.19 and earlier failed to implement access controls on /Stream/ProjectsCSV endpoint, allowing unauthenticated attackers to gain access to potentially sensitive project information stored by the application.	5.3	More Details
CVE-2020-8935	An arbitrary memory overwrite vulnerability in Asylo versions up to 0.6.0 allow an attacker to make an Ecall_restore function call to reallocate untrusted code and overwrite sections of the Enclave memory address. We recommend updating your library.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8941	An arbitrary memory read vulnerability in Asylo versions up to 0.6.0 allows an untrusted attacker to make a call to enc_untrusted_inet_pton using an attacker controlled klinux_addr_buffer parameter. The parameter size is unchecked allowing the attacker to read memory locations outside of the intended buffer size including memory addresses within the secure enclave. We recommend upgrading past commit 8fed5e334131abaf9c5e17307642fbf6ce4a57ec	5.3	More Details
CVE-2020-8940	An arbitrary memory read vulnerability in Asylo versions up to 0.6.0 allows an untrusted attacker to make a call to enc_untrusted_recvmsg using an attacker controlled result parameter. The parameter size is unchecked allowing the attacker to read memory locations outside of the intended buffer size including memory addresses within the secure enclave. We recommend upgrading or past commit fa6485c5d16a7355eab047d4a44345a73bc9131e	5.3	More Details
CVE-2020-8942	An arbitrary memory read vulnerability in Asylo versions up to 0.6.0 allows an untrusted attacker to make a call to enc_untrusted_read whose return size was not validated against the requrested size. The parameter size is unchecked allowing the attacker to read memory locations outside of the intended buffer size including memory addresses within the secure enclave. We recommend upgrading past commit b1d120a2c7d7446d2cc58d517e20a1b184b82200	5.3	More Details
CVE-2020-35460	common/InputStreamHelper.java in Packwood MPXJ before 8.3.5 allows directory traversal in the zip stream handler flow, leading to the writing of files to arbitrary locations.	5.3	More Details
CVE-2020-8936	An arbitrary memory overwrite vulnerability in Asylo versions up to 0.6.0 allows an attacker to make a host call to UntrustedCall. UntrustedCall failed to validate the buffer range within sgx_params and allowed the host to return a pointer that was an address within the enclave memory. This allowed an attacker to read memory values from within the enclave.	5.3	More Details
CVE-2020-8943	An arbitrary memory read vulnerability in Asylo versions up to 0.6.0 allows an untrusted attacker to make a call to enc_untrusted_recvfrom whose return size was not validated against the requested size. The parameter size is unchecked allowing the attacker to read memory locations outside of the intended buffer size including memory addresses within the secure enclave. We recommend upgrading past commit 6e158d558abd3c29a0208e30c97c9a8c5bd4230f	5.3	More Details
CVE-2020-8939	An out of bounds read on the enc_untrusted_inet_ntop function allows an attack to extend the result size that is used by memcpy() to read memory from within the enclave heap. We recommend upgrading past commit 6ff3b77ffe110a33a2f93848a6333f33616f02c4	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8938	An arbitrary memory overwrite vulnerability in Asylo versions up to 0.6.0 allows an attacker to make a host call to FromkLinuxSockAddr with attacker controlled content and size of klinux_addr which allows an attacker to write memory values from within the enclave. We recommend upgrading past commit a37fb6a0e7daf30134dbbf357c9a518a1026aa02	5.3	More Details
CVE-2020-8944	An arbitrary memory write vulnerability in Asylo versions up to 0.6.0 allows an untrusted attacker to make a call to ecall_restore using the attribute output which fails to check the range of a pointer. An attacker can use this pointer to write to arbitrary memory addresses including those within the secure enclave We recommend upgrading past commit 382da2b8b09cbf928668a2445efb778f76bd9c8a	5.3	More Details
CVE-2019-19283	A vulnerability has been identified in XHQ (All Versions < 6.1). The application's web server could expose non-sensitive information about the server's architecture. This could allow an attacker to adapt further attacks to the version in place.	5.3	More Details
CVE-2020-12595	An information disclosure flaw allows a malicious, authenticated, privileged web UI user to obtain a password for a remote SCP backup server that they might not otherwise be authorized to access. This affects SMG prior to 10.7.4.	4.9	More Details
CVE-2020-14302	A flaw was found in Keycloak before 13.0.0 where an external identity provider, after successful authentication, redirects to a Keycloak endpoint that accepts multiple invocations with the use of the same "state" parameter. This flaw allows a malicious user to perform replay attacks.	4.9	More Details
CVE-2020-35126	Typesetter CMS 5.x through 5.1 allows admins to conduct Site Title persistent XSS attacks via an Admin/Configuration URI. NOTE: the significance of this report is disputed because "admins are considered trustworthy.	4.8	More Details
CVE-2020-0473	In updateIncomingFileConfirmNotification of BluetoothOppNotification.java, there is a possible permissions bypass. This could lead to local escalation of privilege allowing an attacker with physical possession of the device to transfer files to it over Bluetooth, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-160691486	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26816	SAP AS JAVA (Key Storage Service), versions - 7.10, 7.11, 7.20 ,7.30, 7.31, 7.40, 7.50, has the key material which is stored in the SAP NetWeaver AS Java Key Storage service stored in the database in the DER encoded format and is not encrypted. This enables an attacker who has administrator access to the SAP NetWeaver AS Java to decode the keys because of missing encryption and get some application data and client credentials of adjacent systems. This highly impacts Confidentiality as information disclosed could contain client credentials of adjacent systems.	4.5	More Details
CVE-2020-27023	In setErrorPlaybackState of BluetoothMediaBrowserService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156009462	4.4	More Details
CVE-2020-27043	In nfc_enabled of nfc_main.cc, there is a possible out of bounds read due to an incorrect increment. This could lead to local information disclosure via firmware with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155234594	4.4	More Details
CVE-2020-27040	In phNxpNciHal_core_initialized of phNxpNciHal.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153731880	4.4	More Details
CVE-2020-26271	In affected versions of TensorFlow under certain cases, loading a saved model can result in accessing uninitialized memory while building the computation graph. The MakeEdge function creates an edge between one output tensor of the src node (given by output_index) and the input slot of the dst node (given by input_index). This is only possible if the types of the tensors on both sides coincide, so the function begins by obtaining the corresponding DataType values and comparing these for equality. However, there is no check that the indices point to inside of the arrays they index into. Thus, this can result in accessing data out of bounds of the corresponding heap allocated arrays. In most scenarios, this can manifest as unitialized data access, but if the index points far away from the boundaries of the arrays this can be used to leak addresses from the library. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0482	In command of IncidentService.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150706572	4.4	More Details
CVE-2020-26268	In affected versions of TensorFlow the tf.raw_ops.ImmutableConst operation returns a constant tensor created from a memory mapped file which is assumed immutable. However, if the type of the tensor is not an integral type, the operation crashes the Python interpreter as it tries to write to the memory area. If the file is too small, TensorFlow properly returns an error as the memory area has fewer bytes than what is needed for the tensor it creates. However, as soon as there are enough bytes, the above snippet causes a segmentation fault. This is because the allocator used to return the buffer data is not marked as returning an opaque handle since the needed virtual method is not overridden. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.	4.4	More Details
CVE-2020-26267	In affected versions of TensorFlow the tf.raw_ops.DataFormatVecPermute API does not validate the src_format and dst_format attributes. The code assumes that these two arguments define a permutation of NHWC. This can result in uninitialized memory accesses, read outside of bounds and even crashes. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.	4.4	More Details
CVE-2020-27021	In avrc_ctrl_pars_vendor_cmd of avrc_pars_tg.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168712245	4.4	More Details
CVE-2020-27037	In phNxpNciHal_core_initialized of phNxpNciHal.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153731335	4.4	More Details
CVE-2020-26270	In affected versions of TensorFlow running an LSTM/GRU model where the LSTM/GRU layer receives an input with zero-length results in a CHECK failure when using the CUDA backend. This can result in a query-of-death vulnerability, via denial of service, if users can control the input to the layer. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26266	In affected versions of TensorFlow under certain cases a saved model can trigger use of uninitialized values during code execution. This is caused by having tensor buffers be filled with the default value of the type but forgetting to default initialize the quantized floating point types in Eigen. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.	4.4	More Details
CVE-2020-27053	In broadcastWifiCredentialChanged of ClientModeImpl.java, there is a possible location permission bypass due to a missing permission check. This could lead to local information disclosure of the WiFi network name with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-159371448	4.4	More Details
CVE-2020-27033	In nfc_ncif_proc_get_routing of nfc_ncif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153655153	4.4	More Details
CVE-2020-27031	In nfc_data_event of nfc_ncif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151313205	4.4	More Details
CVE-2020-0476	In onNotificationRemoved of Assistant.java, there is a possible leak of sensitive information to logs. This could lead to local information disclosure with System execution privileges required. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-162014574	4.4	More Details
CVE-2020-29660	A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.	4.4	More Details
CVE-2020-27028	In filter_incoming_event of hci_layer.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-141618611	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27046	In nfc_ncif_proc_ee_action of nfc_ncif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157649306	4.4	More Details
CVE-2020-26963	Repeated calls to the history and location interfaces could have been used to hang the browser. This was addressed by introducing rate-limiting to these API calls. This vulnerability affects Firefox < 83.	4.3	More Details
CVE-2020-26415	Information about the starred projects for private user profiles was exposed via the GraphQL API starting from 12.2 via the REST API. This affects GitLab >=12.2 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2.	4.3	More Details
CVE-2020-26953	It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.	4.3	More Details
CVE-2020-17153	Microsoft Edge for Android Spoofing Vulnerability	4.3	More Details
CVE-2020-0499	In FLAC__bitreader_read_rice_signed_block of bitreader.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156076070	4.3	More Details
CVE-2020-15376	Brocade Fabric OS versions before v9.0.0 and after version v8.1.0, configured in Virtual Fabric mode contain a weakness in the ldap implementation that could allow a remote ldap user to login in the Brocade Fibre Channel SAN switch with "user" privileges if it is not associated with any groups.	4.3	More Details
CVE-2020-26409	A DOS vulnerability exists in Gitlab CE/EE >=10.3, <13.4.7,>=13.5, <13.5.5,>=13.6, <13.6.2 that allows an attacker to trigger uncontrolled resource by bypassing input validation in markdown fields.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26954	When accepting a malicious intent from other installed apps, Firefox for Android accepted manifests from arbitrary file paths and allowed declaring webapp manifests for other origins. This could be used to gain fullscreen access for UI spoofing and could also lead to cross-origin attacks on targeted websites. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 83.	4.3	More Details
CVE-2020-26411	A potential DOS vulnerability was discovered in all versions of Gitlab starting from 13.4.x (>=13.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2). Using a specific query name for a project search can cause statement timeouts that can lead to a potential DOS if abused.	4.3	More Details
CVE-2020-13357	An issue was discovered in Gitlab CE/EE versions >= 13.1 to <13.4.7, >= 13.5 to <13.5.5, and >= 13.6 to <13.6.2 allowed an unauthorized user to access the user list corresponding to a feature flag in a project.	4.3	More Details
CVE-2020-17131	Chakra Scripting Engine Memory Corruption Vulnerability	4.2	More Details
CVE-2020-26421	Crash in USB HID protocol dissector and possibly other dissectors in Wireshark 3.4.0 and 3.2.0 to 3.2.8 allows denial of service via packet injection or crafted capture file.	4.2	More Details
CVE-2020-26416	Information disclosure in Advanced Search component of GitLab EE starting from 8.4 results in exposure of search terms via Rails logs. This affects versions >=8.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2.	4.0	More Details
CVE-2020-16128	The aptdaemon DBus interface disclosed file existence disclosure by setting Terminal/DebconfSocket properties, aka GHSL-2020-192 and GHSL-2020-196. This affected versions prior to 1.1.1+bzr982-0ubuntu34.1, 1.1.1+bzr982-0ubuntu32.3, 1.1.1+bzr982-0ubuntu19.5, 1.1.1+bzr982-0ubuntu14.5.	3.8	More Details
CVE-2020-29668	Sympa before 6.2.59b.2 allows remote attackers to obtain full SOAP API access by sending any arbitrary string (except one from an expired cookie) as the cookie value to authenticateAndRun.	3.7	More Details
CVE-2020-8284	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28838	Cross Site Request Forgery (CSRF) in CART option in OpenCart Ltd. Opencart CMS 3.0.3.6 allows attacker to add cart items via Add to cart.	3.5	More Details
CVE-2020-8920	An information leak vulnerability exists in Gerrit versions prior to 2.14.22, 2.15.21, 2.16.25, 3.0.15, 3.1.10, 3.2.5 where an overoptimization with the FilteredRepository wrapper skips the verification of access on All-Users repositories, allowing an attacker to get read access to all users' personal information associated with their accounts.	3.5	More Details
CVE-2020-8919	An information leak vulnerability exists in Gerrit versions prior to 2.15.21, 2.16.25, 3.0.15, 3.1.10, 3.2.5 where a missing access check on the branch REST API allows an attacker with only the default set of priviledges to read all other user's personal account data as well as sub-trees with restricted access.	3.5	More Details
CVE-2020-27056	In SELinux policies of mls, there is a missing permission check. This could lead to local information disclosure of package metadata with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-161356067	3.3	More Details
CVE-2020-0459	In sendConfiguredNetworkChangedBroadcast of WifiConfigManager.java, there is a possible leak of sensitive WiFi configuration data due to a missing permission check. This could lead to local information disclosure of WiFi network names with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-159373687	3.3	More Details
CVE-2020-17097	Windows Digital Media Receiver Elevation of Privilege Vulnerability	3.3	More Details
CVE-2020-0481	In AndroidManifest.xml, there is a possible permissions bypass. This could lead to local escalation of privilege allowing a non-system app to send a broadcast it shouldn't have permissions to send, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157472962	3.3	More Details
CVE-2020-27057	In getGpuStatsGlobalInfo and getGpuStatsAppInfo of GpuService.cpp, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure of gpu statistics with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-161903239	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0368	In queryInternal of CallLogProvider.java, there is a possible permission bypass due to improper input validation. This could lead to local information disclosure of voicemail metadata with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-143230980	3.3	More Details
CVE-2020-8908	A temp directory creation vulnerability exists in all versions of Guava, allowing an attacker with access to the machine to potentially access data in a temporary directory created by the Guava API com.google.common.io.Files.createTempDir(). By default, on unix-like systems, the created directory is world-readable (readable by an attacker with access to the system). The method in question has been marked @Deprecated in versions 30.0 and later and should not be used. For Android developers, we recommend choosing a temporary directory API provided by Android, such as context.getCacheDir(). For other Java developers, we recommend migrating to the Java 7 API java.nio.file.Files.createTempDirectory() which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.	3.3	More Details
CVE-2020-26420	Memory leak in RTPS protocol dissector in Wireshark 3.4.0 and 3.2.0 to 3.2.8 allows denial of service via packet injection or crafted capture file.	3.1	More Details
CVE-2020-26419	Memory leak in the dissection engine in Wireshark 3.4.0 allows denial of service via packet injection or crafted capture file.	3.1	More Details
CVE-2020-26418	Memory leak in Kafka protocol dissector in Wireshark 3.4.0 and 3.2.0 to 3.2.8 allows denial of service via packet injection or crafted capture file.	3.1	More Details
CVE-2020-26412	Removed group members were able to use the To-Do functionality to retrieve updated information on confidential epics starting in GitLab EE 13.2 before 13.6.2.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-29480	An issue was discovered in Xen through 4.14.x. Neither xenstore implementation does any permission checks when reporting a xenstore watch event. A guest administrator can watch the root xenstored node, which will cause notifications for every created, modified, and deleted key. A guest administrator can also use the special watches, which will cause a notification every time a domain is created and destroyed. Data may include: number, type, and domids of other VMs; existence and domids of driver domains; numbers of virtual interfaces, block devices, vcpus; existence of virtual framebuffers and their backend style (e.g., existence of VNC service); Xen VM UUIDs for other domains; timing information about domain creation and device setup; and some hints at the backend provisioning of VMs and their devices. The watch events do not contain values stored in xenstore, only key names. A guest administrator can observe non-sensitive domain and device lifecycle events relating to other guests. This information allows some insight into overall system configuration (including the number and general nature of other guests), and configuration of other guests (including the number and general nature of other guests' devices). This information might be commercially interesting or might make other attacks easier. There is not believed to be exposure of sensitive data. Specifically, there is no exposure of VNC passwords, port numbers, pathnames in host and guest filesystems, cryptographic keys, or within-guest data.	2.3	More Details
CVE-2020-27351	Various memory and file descriptor leaks were found in apt-python files python/arfile.cc, python/tag.cc, python/tarfile.cc, aka GHSL-2020-170. This issue affects: python-apt 1.1.0~beta1 versions prior to 1.1.0~beta1ubuntu0.16.04.10; 1.6.5ubuntu0 versions prior to 1.6.5ubuntu0.4; 2.0.0ubuntu0 versions prior to 2.0.0ubuntu0.20.04.2; 2.1.3ubuntu1 versions prior to 2.1.3ubuntu1.1;	2.0	More Details
CVE-2020-2086	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35110	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-2020-25707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate is a duplicate of CVE-2020-2891	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-16598	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-29606	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-2089	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-2088	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-2087	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-16196	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-2085	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-29589	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-5021. Reason: This candidate is a reservation duplicate of CVE-2019-5021. Notes: All CVE users should reference CVE-2019-5021 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-0487	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-2020-9001	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8999	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-17160	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-2020-21009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2016-15001	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-2020-35144	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-29590	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-5021. Reason: This candidate is a reservation duplicate of CVE-2019-5021. Notes: All CVE users should reference CVE-2019-5021 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-2084	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35076	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-2020-35090	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-2020-2079	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2080	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-2081	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-2082	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-2083	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2020. Notes: none	N/A	More Details
CVE-2020-35465	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details