SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 May 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-2020-13126	An issue was discovered in the Elementor Pro plugin before 2.9.4 for WordPress, as exploited in the wild in May 2020 in conjunction with CVE-2020-13125. An attacker with the Subscriber role can upload arbitrary executable files to achieve remote code execution. NOTE: the free Elementor plugin is unaffected.	9.9	More Details
CVE-2020-10654	Ping Identity PingID SSH before 4.0.14 contains a heap buffer overflow in PingID-enrolled servers. This condition can be potentially exploited into a Remote Code Execution vector on the authenticating endpoint.	9.8	More Details
CVE-2020-12889	MISP MISP-maltego 1.4.4 incorrectly shares a MISP connection across users in a remote-transform use case.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13091	pandas through 1.0.3 can unserialize and execute commands from an untrusted file that is passed to the read_pickle() function, if __reduce__ makes an os.system call. NOTE: third parties dispute this issue because the read_pickle() function is documented as unsafe and it is the user's responsibility to use the function in a secure manner	9.8	More Details
CVE-2020-13092	scikit-learn (aka sklearn) through 0.23.0 can unserialize and execute commands from an untrusted file that is passed to the joblib.load() function, if __reduce__ makes an os.system call. NOTE: third parties dispute this issue because the joblib.load() function is documented as unsafe and it is the user's responsibility to use the function in a secure manner	9.8	More Details
CVE-2020-8149	Lack of output sanitization allowed an attack to execute arbitrary shell commands via the logkitty npm package before version 0.7.1.	9.8	More Details
CVE-2020-13109	Morita Shogi 64 through 2020-05-02 for Nintendo 64 devices allows remote attackers to execute arbitrary code via crafted packet data to the built-in modem because 0x800b3e94 (aka the IF subcommand to top-level command 7) has a stack-based buffer overflow.	9.8	More Details
CVE-2020-13118	An issue was discovered in Mikrotik-Router-Monitoring-System through 2018-10-22. SQL Injection exists in check_community.php via the parameter community.	9.8	More Details
CVE-2019-20800	In Cherokee through 1.2.104, remote attackers can trigger an out-of-bounds write in cherokee_handler_cgi_add_env_pair in handler_cgi.c by sending many request headers, as demonstrated by a GET request with many "Host: 127.0.0.1" headers.	9.8	More Details
CVE-2020-12763	TRENDnet ProView Wireless camera TV-IP512WN 1.0R 1.0.4 is vulnerable to an unauthenticated stack-based buffer overflow in handling RTSP packets. This may result in remote code execution or denial of service. The issue is in the binary rtspd (in /sbin) when parsing a long "Authorization: Basic" RTSP header.	9.8	More Details
CVE-2020-12856	OpenTrace, as used in COVIDSafe through v1.0.17, TraceTogether, ABTraceTogether, and other applications on iOS and Android, allows remote attackers to conduct long-term re-identification attacks and possibly have unspecified other impact, because of how Bluetooth is used.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-7247	An issue was discovered in AODDriver2.sys in AMD OverDrive. The vulnerable driver exposes a wrmsr instruction via IOCTL 0x81112ee0 and does not properly filter the Model Specific Register (MSR). Allowing arbitrary MSR writes can lead to Ring-0 code execution and escalation of privileges.	9.8	More Details
CVE-2020-1897	A use-after-free is possible due to an error in lifetime management in the request adaptor when a malicious client invokes request error handling in a specific sequence. This issue affects versions of proxygen prior to v2020.05.18.00.	9.8	More Details
CVE-2020-8434	Jenzabar JICS (aka Internet Campus Solution) before 9.0.1 Patch 3, 9.1 before 9.1.2 Patch 2, and 9.2 before 9.2.2 Patch 8 has session cookies that are a deterministic function of the username. There is a hard-coded password to supply a PBKDF feeding into AES to encrypt a username and base64 encode it to a client-side cookie for persistent session authentication. By knowing the key and algorithm, an attacker can select any username, encrypt it, base64 encode it, and save it in their browser with the correct JICSLoginCookie cookie format to impersonate any real user in the JICS database without the need for authenticating (or verifying with MFA if implemented).	9.8	More Details
CVE-2020-11715	Panasonic P99 devices through 2020-04-10 have Incorrect Access Control. NOTE: the vendor states that all affected products are at "End-of-software-support."	9.8	More Details
CVE-2020-13166	The management tool in MyLittleAdmin 3.8 allows remote attackers to execute arbitrary code because machineKey is hardcoded (the same for all customers' installations) in web.config, and can be used to send serialized ASP code.	9.8	More Details
CVE-2020-12651	SecureCRT before 8.7.2 allows remote attackers to execute arbitrary code via an Integer Overflow and a Buffer Overflow because a banner can trigger a line number to CSI functions that exceeds INT_MAX.	9.8	More Details
CVE-2019-18666	An issue was discovered on D-Link DAP-1360 revision F devices. Remote attackers can start a telnet service without authorization via an undocumented HTTP request. Although this is the primary vulnerability, the impact depends on the firmware version. Versions 609EU through 613EUbeta were tested. Versions through 6.12b01 have weak root credentials, allowing an attacker to gain remote root access. After 6.12b01, the root credentials were changed but the telnet service can still be started without authorization.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12834	eQ-3 Homematic Central Control Unit (CCU)2 through 2.51.6 and CCU3 through 3.51.6 allow Remote Code Execution in the JSON API Method ReGa.runScript, by unauthenticated attackers with access to the web interface, due to the default auto-login feature being enabled during first-time setup (or factory reset).	9.8	More Details
CVE-2020-11972	Apache Camel RabbitMQ enables Java deserialization by default. Apache Camel 2.22.x, 2.23.x, 2.24.x, 2.25.0, 3.0.0 up to 3.1.0 are affected. 2.x users should upgrade to 2.25.1, 3.x users should upgrade to 3.2.0.	9.8	More Details
CVE-2019-15880	In FreeBSD 12.1-STABLE before r356911, and 12.1-RELEASE before p5, insufficient checking in the cryptodev module allocated the size of a kernel buffer based on a user-supplied length allowing an unprivileged process to trigger a kernel panic.	9.8	More Details
CVE-2020-7454	In FreeBSD 12.1-STABLE before r360971, 12.1-RELEASE before p5, 11.4-STABLE before r360971, 11.4-BETA1 before p1 and 11.3-RELEASE before p9, libalias does not properly validate packet length resulting in modules causing an out of bounds read/write condition if no checking was built into the module.	9.8	More Details
CVE-2020-9502	Some Dahua products with Build time before December 2019 have Session ID predictable vulnerabilities. During normal user access, an attacker can use the predicted Session ID to construct a data packet to attack the device.	9.8	More Details
CVE-2020-12832	WordPress Plugin Simple File List before 4.2.8 is prone to a vulnerability that lets attackers delete arbitrary files because the application fails to properly verify user-supplied input.	9.8	More Details
CVE-2019-13022	Bond JetSelect (all versions) has an issue in the Java class (ENCtool.jar) and corresponding password generation algorithm (used to set initial passwords upon first installation). It XORs the plaintext into the 'encrypted' password that is then stored within the database. These steps are able to be trivially reversed, allowing for escalation of privilege within the JetSelect application through obtaining the passwords of JetSelect administrators. JetSelect administrators have the ability to modify and delete all networking configuration across a vessel, as well as altering network configuration of all managed network devices (switches, routers).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-17562	A buffer overflow vulnerability has been found in the baremetal component of Apache CloudStack. This applies to all versions prior to 4.13.1. The vulnerability is due to the lack of validation of the mac parameter in baremetal virtual router. If you insert an arbitrary shell command into the mac parameter, v-router will process the command. For example: Normal: http://{GW}:10086/baremetal/provisiondone/{mac}, Abnormal: http://{GW}:10086/baremetal/provisiondone/#';whoami;#. Mitigation of this issue is an upgrade to Apache CloudStack 4.13.1.0 or beyond.	9.8	More Details
CVE-2020-11973	Apache Camel Netty enables Java deserialization by default. Apache Camel 2.22.x, 2.23.x, 2.24.x, 2.25.0, 3.0.0 up to 3.1.0 are affected. 2.x users should upgrade to 2.25.1, 3.x users should upgrade to 3.2.0.	9.8	More Details
CVE-2020-12874	Veritas APTARE versions prior to 10.4 included code that bypassed the normal login process when specific authentication credentials were provided to the server.	9.8	More Details
CVE-2020-0103	In a2dp_aac_decoder_cleanup of a2dp_aac_decoder.cc, there is a possible invalid free due to memory corruption. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-9Android ID: A-148107188	9.8	More Details
CVE-2020-0221	Airbrush FW's scratch memory allocator is susceptible to numeric overflow. When the overflow occurs, the next allocation could potentially return a pointer within the previous allocation's memory, which could lead to improper memory access.Product: AndroidVersions: Android kernelAndroid ID: A-135772851	9.8	More Details
CVE-2020-10620	Opto 22 SoftPAC Project Version 9.6 and prior. SoftPAC communication does not include any credentials. This allows an attacker with network access to directly communicate with SoftPAC, including, for example, stopping the service remotely.	9.8	More Details
CVE-2020-13167	Netsweeper through 6.4.3 allows unauthenticated remote code execution because webadmin/tools/unixlogin.php (with certain Referer headers) launches a command line with client-supplied parameters, and allows injection of shell metacharacters.	9.8	More Details
CVE-2020-12258	rConfig 3.9.4 is vulnerable to session fixation because session expiry and randomization are mishandled. The application can reuse a session via PHPSESSID. Also, an attacker can exploit this vulnerability in conjunction with CVE-2020-12256 or CVE-2020-12259.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10612	Opto 22 SoftPAC Project Version 9.6 and prior. SoftPACAgent communicates with SoftPACMonitor over network Port 22000. However, this port is open without any restrictions. This allows an attacker with network access to control the SoftPACAgent service including updating SoftPAC firmware, starting or stopping service, or writing to certain registry values.	9.1	More Details
CVE-2020-8100	Improper Input Validation vulnerability in the cevakrnl.rv0 module as used in the Bitdefender Engines allows an attacker to trigger a denial of service while scanning a specially-crafted sample. This issue affects: Bitdefender Bitdefender Engines versions prior to 7.84063.	9.0	More Details
CVE-2020-2018	An authentication bypass vulnerability in the Panorama context switching feature allows an attacker with network access to a Panorama's management interface to gain privileged access to managed firewalls. An attacker requires some knowledge of managed firewalls to exploit this issue. This issue does not affect Panorama configured with custom certificates authentication for communication between Panorama and managed devices. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.12; PAN-OS 9.0 versions earlier than 9.0.6; All versions of PAN-OS 8.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-10616	Opto 22 SoftPAC Project Version 9.6 and prior. SoftPAC does not specify the path of multiple imported .dll files. Therefore, an attacker can replace them and execute code whenever the service starts.	8.8	More Details
CVE-2020-2015	A buffer overflow vulnerability in the PAN-OS management server allows authenticated users to crash system processes or potentially execute arbitrary code with root privileges. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.7; PAN-OS 9.1 versions earlier than 9.1.1; All versions of PAN-OS 8.0.	8.8	More Details
CVE-2020-12255	rConfig 3.9.4 is vulnerable to remote code execution due to improper validation in the file upload functionality. vendor.crud.php accepts a file upload by checking content-type without considering the file extension and header. Thus, an attacker can exploit this by uploading a .php file to vendor.php that contains arbitrary PHP code and changing the content-type to image/gif.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5407	Spring Security versions 5.2.x prior to 5.2.4 and 5.3.x prior to 5.3.2 contain a signature wrapping vulnerability during SAML response validation. When using the spring-security-saml2-service-provider component, a malicious user can carefully modify an otherwise valid SAML response and append an arbitrary assertion that Spring Security will accept as valid.	8.8	More Details
CVE-2020-11549	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system.	8.8	More Details
CVE-2020-11551	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc.	8.8	More Details
CVE-2020-6074	An exploitable code execution vulnerability exists in the PDF parser of Nitro Pro 13.9.1.155. A specially crafted PDF document can cause a use-after-free which can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.8	More Details
CVE-2020-2017	A DOM-Based Cross Site Scripting Vulnerability exists in PAN-OS and Panorama Management Web Interfaces. A remote attacker able to convince an authenticated administrator to click on a crafted link to PAN-OS and Panorama Web Interfaces could execute arbitrary JavaScript code in the administrator's browser and perform administrative actions. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; All versions of PAN-OS 8.0.	8.8	More Details
CVE-2020-1714	A flaw was found in Keycloak before version 11.0.0, where the code base contains usages of ObjectInputStream without type checks. This flaw allows an attacker to inject arbitrarily serialized Java Objects, which would then get deserialized in a privileged context and potentially lead to remote code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13144	Studio in Open edX Ironwood 2.5, when CodeJail is not used, allows a user to go to the "Create New course>New section>New subsection>New unit>Add new component>Problem button>Advanced tab>Custom Python evaluated code" screen, edit the problem, and execute Python code. This leads to arbitrary code execution.	8.8	More Details
CVE-2020-13146	Studio in Open edX Ironwood 2.5 allows CSV injection because an added cohort in Course>Instructor>Cohorts may contain a formula that is exported via the "Course>Data Downloads>Reports>Download profile info" feature.	8.8	More Details
CVE-2020-11067	In TYPO3 CMS 9.0.0 through 9.5.16 and 10.0.0 through 10.4.1, it has been discovered that backend user settings (in $BE_USER->uc) are vulnerable to insecure deserialization. In combination with vulnerabilities of third party components, this can lead to remote code execution. A valid backend user account is needed to exploit this vulnerability. This has been fixed in 9.5.17 and 10.4.2.	8.8	More Details
CVE-2020-12427	The Western Digital WD Discovery application before 3.8.229 for MyCloud Home on Windows and macOS is vulnerable to CSRF, with impacts such as stealing data, modifying disk contents, or exhausting disk space.	8.8	More Details
CVE-2019-16112	TylerTech Eagle 2018.3.11 deserializes untrusted user input, resulting in remote code execution via a crafted Java object to the recorder/ServiceManager?service=tyler.empire.settings.SettingManager URI.	8.8	More Details
CVE-2020-5576	Cross-site request forgery (CSRF) vulnerability in Movable Type series (Movable Type 7 r.4606 (7.2.1) and earlier (Movable Type 7), Movable Type Advanced 7 r.4606 (7.2.1) and earlier (Movable Type Advanced 7), Movable Type for AWS 7 r.4606 (7.2.1) and earlier (Movable Type for AWS 7), Movable Type 6.5.3 and earlier (Movable Type 6.5), Movable Type Advanced 6.5.3 and earlier (Movable Type Advanced 6.5), Movable Type 6.3.11 and earlier (Movable Type 6.3), Movable Type Advanced 6.3.11 and earlier (Movable Type 6.3), Movable Type Premium 1.29 and earlier, and Movable Type Premium Advanced 1.29 and earlier) allows remote attackers to hijack the authentication of administrators via unspecified vectors.	8.8	More Details
CVE-2020-2014	An OS Command Injection vulnerability in PAN-OS management server allows authenticated users to inject and execute arbitrary shell commands with root privileges. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10030	An issue has been found in PowerDNS Recursor 4.1.0 up to and including 4.3.0. It allows an attacker (with enough privileges to change the system's hostname) to cause disclosure of uninitialized memory content via a stack-based out-of-bounds read. It only occurs on systems where gethostname() does not have '\0' termination of the returned string if the hostname is larger than the supplied buffer. (Linux systems are not affected because the buffer is always large enough. OpenBSD systems are not affected because the returned hostname always has '\0' termination.) Under some conditions, this issue can lead to the writing of one '\0' byte out-of-bounds on the stack, causing a denial of service or possibly arbitrary code execution.	8.8	More Details
CVE-2020-5577	Movable Type series (Movable Type 7 r.4606 (7.2.1) and earlier (Movable Type 7), Movable Type Advanced 7 r.4606 (7.2.1) and earlier (Movable Type Advanced 7), Movable Type for AWS 7 r.4606 (7.2.1) and earlier (Movable Type for AWS 7), Movable Type 6.5.3 and earlier (Movable Type 6.5), Movable Type Advanced 6.5.3 and earlier (Movable Type Advanced 6.5), Movable Type 6.3.11 and earlier (Movable Type 6.3), Movable Type Advanced 6.3.11 and earlier (Movable Type 6.3), Movable Type Premium 1.29 and earlier, and Movable Type Premium Advanced 1.29 and earlier) allow remote authenticated attackers to upload arbitrary files and execute a php script via unspecified vectors.	8.8	More Details
CVE-2020-11766	sendfax.php in iFAX AvantFAX before 3.3.6 and HylaFAX Enterprise Web Interface before 0.2.5 allows authenticated Command Injection.	8.8	More Details
CVE-2020-2025	Kata Containers before 1.11.0 on Cloud Hypervisor persists guest filesystem changes to the underlying image file on the host. A malicious guest can overwrite the image file to gain control of all subsequent guest VMs. Since Kata Containers uses the same VM image file with all VMMs, this issue may also affect QEMU and Firecracker based guests.	8.8	More Details
CVE-2020-7138	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100	8.8	More Details
CVE-2020-12257	rConfig 3.9.4 is vulnerable to cross-site request forgery (CSRF) because it lacks implementation of CSRF protection such as a CSRF token. An attacker can leverage this vulnerability by creating a form (add a user, delete a user, or edit a user).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11066	In TYPO3 CMS greater than or equal to 9.0.0 and less than 9.5.17 and greater than or equal to 10.0.0 and less than 10.4.2, calling unserialize() on malicious user-submitted content can lead to modification of dynamically-determined object attributes and result in triggering deletion of an arbitrary directory in the file system, if it is writable for the web server. It can also trigger message submission via email using the identity of the web site (mail relay). Another insecure deserialization vulnerability is required to actually exploit mentioned aspects. This has been fixed in 9.5.17 and 10.4.2.	8.7	More Details
CVE-2020-8616	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.	8.6	More Details
CVE-2019-20798	An XSS issue was discovered in handler_server_info.c in Cherokee through 1.2.104. The requested URL is improperly displayed on the About page in the default configuration of the web server and its administrator panel. The XSS in the administrator panel can be used to reconfigure the server and execute arbitrary commands.	8.4	More Details
CVE-2020-2013	A cleartext transmission of sensitive information vulnerability in Palo Alto Networks PAN-OS Panorama that discloses an authenticated PAN-OS administrator's PAN-OS session cookie. When an administrator issues a context switch request into a managed firewall with an affected PAN-OS Panorama version, their PAN-OS session cookie is transmitted over cleartext to the firewall. An attacker with the ability to intercept this network traffic between the firewall and Panorama can access the administrator's account and further manipulate devices managed by Panorama. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; PAN-OS 9.1 versions earlier than 9.1.1; All version of PAN-OS 8.0;	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2001	An external control of path and data vulnerability in the Palo Alto Networks PAN-OS Panorama XSLT processing logic that allows an unauthenticated user with network access to PAN-OS management interface to write attacker supplied file on the system and elevate privileges. This issue affects: All PAN-OS 7.1 Panorama and 8.0 Panorama versions; PAN-OS 8.1 versions earlier than 8.1.12 on Panorama; PAN-OS 9.0 versions earlier than 9.0.6 on Panorama.	8.1	More Details
CVE-2020-7139	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100	8.1	More Details
CVE-2020-2002	An authentication bypass by spoofing vulnerability exists in the authentication daemon and User-ID components of Palo Alto Networks PAN-OS by failing to verify the integrity of the Kerberos key distribution center (KDC) before authenticating users. This affects all forms of authentication that use a Kerberos authentication profile. A man-in-the-middle type of attacker with the ability to intercept communication between PAN-OS and KDC can login to PAN-OS as an administrator. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; All version of PAN-OS 8.0.	8.1	More Details
CVE-2019-20390	A Cross-Site Request Forgery (CSRF) vulnerability was discovered in Subrion CMS 4.2.1 that allows a remote attacker to remove files on the server without a victim's knowledge, by enticing an authenticated user to visit an attacker's web page. The application fails to validate the CSRF token for a GET request. An attacker can craft a panel/uploads/read.json?cmd=rm URL (removing this token) and send it to the victim.	8.1	More Details
CVE-2019-9682	Dahua devices with Build time before December 2019 use strong security login mode by default, but in order to be compatible with the normal login of early devices, some devices retain the weak security login mode that users can control. If the user uses a weak security login method, an attacker can monitor the device network to intercept network packets to attack the device. So it is recommended that the user disable this login method.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11069	In TYPO3 CMS 9.0.0 through 9.5.16 and 10.0.0 through 10.4.1, it has been discovered that the backend user interface and install tool are vulnerable to a same-site request forgery. A backend user can be tricked into interacting with a malicious resource an attacker previously managed to upload to the web server. Scripts are then executed with the privileges of the victims' user session. In a worst-case scenario, new admin users can be created which can directly be used by an attacker. The vulnerability is basically a cross-site request forgery (CSRF) triggered by a cross-site scripting vulnerability (XSS) - but happens on the same target host - thus, it's actually a same-site request forgery. Malicious payload such as HTML containing JavaScript might be provided by either an authenticated backend user or by a non-authenticated user using a third party extension, e.g. file upload in a contact form with knowing the target location. To be successful, the attacked victim requires an active and valid backend or install tool user session at the time of the attack. This has been fixed in 9.5.17 and 10.4.2. The deployment of additional mitigation techniques is suggested as described below. - Sudo Mode Extension This TYPO3 extension intercepts modifications to security relevant database tables, e.g. those storing user accounts or storages of the file abstraction layer. Modifications need to confirmed again by the acting user providing their password again. This technique is known as sudo mode. This way, unintended actions happening in the background can be mitigated. - https://github.com/FriendsOfTYPO3/sudo-mode - https://extensions.typo3.org/extension/sudo_mode - Content Security Policy Content Security Policies tell (modern) browsers how resources served a particular site are handled. It is also possible to disallow script executions for specific locations. In a TYPO3 context, it is suggested to disallow direct script execution at least for locations /fileadmin/ and /uploads/.	8.0	More Details
CVE-2020-11073	In Autoswitch Python Virtualenv before version 0.16.0, a user who enters a directory with a malicious `.venv` file could run arbitrary code without any user interaction. This is fixed in version: 1.16.0	7.9	More Details
CVE-2018-10756	Use-after-free in libtransmission/variant.c in Transmission before 3.00 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted torrent file.	7.8	More Details
CVE-2020-4285	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by a memory corruption error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash. IBM X-Force ID: 176266	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4288	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by a memory corruption error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash. IBM X-Force ID: 176270.	7.8	More Details
CVE-2020-13149	Weak permissions on the "%PROGRAMDATA%\MSI\Dragon Center" folder in Dragon Center before 2.6.2003.2401, shipped with Micro-Star MSI Gaming laptops, allows local authenticated users to overwrite system files and gain escalated privileges. One attack method is to change the Recommended App binary within App.json. Another attack method is to use this part of %PROGRAMDATA% for mounting an RPC Control directory.	7.8	More Details
CVE-2020-4287	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by a memory corruption error. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash. IBM X-Force ID: 176269.	7.8	More Details
CVE-2020-4266	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175649.	7.8	More Details
CVE-2020-4422	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially crafted file, a remote attacker could exploit this vulnerability to execute arbitrary code on the system or cause the application to crash. IBM X-Force ID: 180167.	7.8	More Details
CVE-2019-17066	In Ivanti WorkSpace Control before 10.4.40.0, a user can elevate rights on the system by hijacking certain user registries. This is possible because pwrgrid.exe first checks the Current User registry hives (HKCU) when starting an application with elevated rights.	7.8	More Details
CVE-2020-11807	Because of Unrestricted Upload of a File with a Dangerous Type, Sourcefabric Newscoop 4.4.7 allows an authenticated user to execute arbitrary PHP code (and sometimes terminal commands) on a server by making an avatar update and then visiting the avatar file under the /images/ path.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4264	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175647.	7.8	More Details
CVE-2020-4263	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175646.	7.8	More Details
CVE-2020-4262	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175645.	7.8	More Details
CVE-2020-4343	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially crafted file, a remote attacker could exploit this vulnerability to execute arbitrary code on the system or cause the application to crash. IBM X-Force ID: 178244.	7.8	More Details
CVE-2020-4467	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by memory corruption. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash. IBM X-Force ID: 181721.	7.8	More Details
CVE-2020-6092	An exploitable code execution vulnerability exists in the way Nitro Pro 13.9.1.155 parses Pattern objects. A specially crafted PDF file can trigger an integer overflow that can lead to arbitrary code execution. In order to trigger this vulnerability, victim must open a malicious file.	7.8	More Details
CVE-2019-19721	An off-by-one error in the DecodeBlock function in codec/sdl_image.c in VideoLAN VLC media player before 3.0.9 allows remote attackers to cause a denial of service (memory corruption) via a crafted image file. NOTE: this may be related to the SDL_Image product.	7.8	More Details
CVE-2020-13110	The kerberos package before 1.0.0 for Node.js allows arbitrary code execution and privilege escalation via injection of malicious DLLs through use of the kerberos_sspi LoadLibrary() method, because of a DLL path search.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12798	Cellebrite UFED 5.0 to 7.5.0.845 implements local operating system policies that can be circumvented to obtain a command prompt via the Windows file dialog that is reachable via the Certificate-Based Authentication option of the Wireless Network Connection screen.	7.8	More Details
CVE-2020-4468	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a remote attacker to execute arbitrary code on the system, caused by memory corruption. By persuading a victim to open a specially-crafted document, a remote attacker could exploit this vulnerability to execute arbitrary code on the system with the privileges of the victim or cause the application to crash. IBM X-Force ID: 181723.	7.8	More Details
CVE-2020-0024	In onCreate of SettingsBaseActivity.java, there is a possible unauthorized setting modification due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-137015265	7.8	More Details
CVE-2020-0094	In setImageHeight and setImageWidth of ExifUtils.cpp, there is a possible out of bounds write due to an incorrect 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-9 Android-10Android ID: A-148223871	7.8	More Details
CVE-2020-0096	In startActivities of ActivityStartController.java, there is a possible escalation of privilege due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-145669109	7.8	More Details
CVE-2020-0097	In various methods of PackageManagerService.java, there is a possible permission bypass due to a missing condition for system apps. This could lead to local escalation of privilege with User privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-145981139	7.8	More Details
CVE-2020-0098	In navigateUpToLocked of ActivityStack.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.0 Android-8.1 Android-9Android ID: A-144285917	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0102	In GattServer::SendResponse of gatt_server.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-143231677	7.8	More Details
CVE-2020-0105	In onKeyguardVisibilityChanged of key_store_service.cpp, there is a missing permission check. This could lead to local escalation of privilege, allowing apps to use keyguard-bound keys when the screen is locked, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144285084	7.8	More Details
CVE-2020-0109	In simulatePackageSuspendBroadcast of NotificationManagerService.java, there is a missing permission check. This could lead to local escalation of privilege by creating fake system notifications with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-148059175	7.8	More Details
CVE-2020-4258	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175637.	7.8	More Details
CVE-2020-4261	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175644.	7.8	More Details
CVE-2020-0110	In psi_write of psi.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-148159562References: Upstream kernel	7.8	More Details
CVE-2020-4257	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175635.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10626	In Fazecast jSerialComm, Version 2.2.2 and prior, an uncontrolled search path element vulnerability could allow a malicious DLL file with the same name of any resident DLLs inside the software installation to execute arbitrary code.	7.8	More Details
CVE-2019-15878	In FreeBSD 12.1-STABLE before r352509, 11.3-STABLE before r352509, and 11.3-RELEASE before p9, an unprivileged local user can trigger a use-after-free situation due to improper checking in SCTP when an application tries to update an SCTP-AUTH shared key.	7.8	More Details
CVE-2020-3341	A vulnerability in the PDF archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.101 - 0.102.2 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a stack buffer overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	7.5	More Details
CVE-2019-19454	An arbitrary file download was found in the "Download Log" functionality of Wowza Streaming Engine <= 4.x.x. This issue was resolved in Wowza Streaming Engine 4.8.0.	7.5	More Details
CVE-2020-2011	An improper input validation vulnerability in the configuration daemon of Palo Alto Networks PAN-OS Panorama allows for a remote unauthenticated user to send a specifically crafted registration request to the device that causes the configuration service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS Panorama services by restarting the device and putting it into maintenance mode. This issue affects: All versions of PAN-OS 7.1, PAN-OS 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7; PAN-OS 9.1 versions earlier than 9.1.0.	7.5	More Details
CVE-2020-3327	A vulnerability in the ARJ archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.102.2 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a heap buffer overflow read. An attacker could exploit this vulnerability by sending a crafted ARJ file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	7.5	More Details
CVE-2019-20797	An issue was discovered in e6y prboom-plus 2.5.1.5. There is a buffer overflow in client and server code responsible for handling received UDP packets, as demonstrated by I_SendPacket or I_SendPacketTo in i_network.c.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20799	In Cherokee through 1.2.104, multiple memory corruption errors may be used by a remote attacker to destabilize the work of a server.	7.5	More Details
CVE-2020-13128	An issue was discovered in Manolo GWTUpload 1.0.3. server/UploadServlet.java (the servlet for handling file upload) accepts a delay parameter that causes a thread to sleep. It can be abused to cause all of a server's threads to sleep, leading to denial of service.	7.5	More Details
CVE-2020-12857	Caching of GATT characteristic values (TempID) in COVIDSafe v1.0.15 and v1.0.16 allows a remote attacker to long-term re-identify an Android device running COVIDSafe.	7.5	More Details
CVE-2020-12858	Non-reinitialisation of random data in the advertising payload in COVIDSafe v1.0.15 and v1.0.16 allows a remote attacker to re-identify Android devices running COVIDSafe by scanning for their advertising beacons.	7.5	More Details
CVE-2020-10957	In Dovecot before 2.3.10.1, unauthenticated sending of malformed parameters to a NOOP command causes a NULL Pointer Dereference and crash in submission-login, submission, or lmtp.	7.5	More Details
CVE-2020-13136	D-Link DSP-W215 1.26b03 devices send an obfuscated hash that can be retrieved and understood by a network sniffer.	7.5	More Details
CVE-2020-13164	In Wireshark 3.2.0 to 3.2.3, 3.0.0 to 3.0.10, and 2.6.0 to 2.6.16, the NFS dissector could crash. This was addressed in epan/dissectors/packet-nfs.c by preventing excessive recursion, such as for a cycle in the directory graph on a filesystem.	7.5	More Details
CVE-2020-12876	Veritas APTARE versions prior to 10.4 allowed remote users to access several unintended files on the server. This vulnerability only impacts Windows server deployments.	7.5	More Details
CVE-2020-12667	Knot Resolver before 5.1.1 allows traffic amplification via a crafted DNS answer from an attacker-controlled server, aka an "NXNSAttack" issue. This is triggered by random subdomains in the NSDNAME in NS records.	7.5	More Details
CVE-2020-12244	An issue has been found in PowerDNS Recursor 4.1.0 through 4.3.0 where records in the answer section of a NXDOMAIN response lacking an SOA were not properly validated in SyncRes::processAnswer, allowing an attacker to bypass DNSSEC validation.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12662	Unbound before 1.10.1 has Insufficient Control of Network Message Volume, aka an "NXNSAttack" issue. This is triggered by random subdomains in the NSDNAME in NS records.	7.5	More Details
CVE-2020-12663	Unbound before 1.10.1 has an infinite loop via malformed DNS answers received from upstream servers.	7.5	More Details
CVE-2020-8617	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results.	7.5	More Details
CVE-2020-1695	A flaw was found in all resteasy 3.x.x versions prior to 3.12.0.Final and all resteasy 4.x.x versions prior to 4.6.0.Final, where an improper input validation results in returning an illegal header that integrates into the server's response. This flaw may result in an injection, which leads to unexpected behavior when the HTTP response is constructed.	7.5	More Details
CVE-2020-10995	PowerDNS Recursor from 4.1.0 up to and including 4.3.0 does not sufficiently defend against amplification attacks. An issue in the DNS protocol has been found that allow malicious parties to use recursive DNS services to attack third party authoritative name servers. The attack uses a crafted reply by an authoritative name server to amplify the resulting traffic between the recursive and other authoritative name servers. Both types of service can suffer degraded performance as an effect. This is triggered by random subdomains in the NSDNAME in NS records. PowerDNS Recursor 4.1.16, 4.2.2 and 4.3.1 contain a mitigation to limit the impact of this DNS protocol issue.	7.5	More Details
CVE-2020-12877	Veritas APTARE versions prior to 10.4 allowed sensitive information to be accessible without authentication.	7.5	More Details
CVE-2020-13111	NaviServer 4.99.4 to 4.99.19 allows denial of service due to the nsd/driver.c ChunkedDecode function not properly validating the length of a chunk. A remote attacker can craft a chunked-transfer request that will result in a negative value being passed to memmove via the size parameter, causing the process to crash.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2012	Improper restriction of XML external entity reference ('XXE') vulnerability in Palo Alto Networks Panorama management service allows remote unauthenticated attackers with network access to the Panorama management interface to read arbitrary files on the system. This issue affects: All versions of PAN-OS for Panorama 7.1 and 8.0; PAN-OS for Panorama 8.1 versions earlier than 8.1.13; PAN-OS for Panorama 9.0 versions earlier than 9.0.7.	7.5	More Details
CVE-2020-11971	Apache Camel's JMX is vulnerable to Rebind Flaw. Apache Camel 2.22.x, 2.23.x, 2.24.x, 2.25.x, 3.0.0 up to 3.1.0 is affected. Users should upgrade to 3.2.0.	7.5	More Details
CVE-2020-13163	em-imap 0.5 uses the library eventmachine in an insecure way that allows an attacker to perform a man-in-the-middle attack against users of the library. The hostname in a TLS server certificate is not verified.	7.4	More Details
CVE-2019-15879	In FreeBSD 12.1-STABLE before r356908, 12.1-RELEASE before p5, 11.3-STABLE before r356908, and 11.3-RELEASE before p9, a race condition in the cryptodev module permitted a data structure in the kernel to be used after it was freed, allowing an unprivileged process can overwrite arbitrary kernel memory.	7.4	More Details
CVE-2020-4265	IBM i2 Intelligent Analyis Platform 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 175648.	7.3	More Details
CVE-2020-2010	An OS command injection vulnerability in PAN-OS management interface allows an authenticated administrator to execute arbitrary OS commands with root privileges. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	7.2	More Details
CVE-2020-2008	An OS command injection and external control of filename vulnerability in Palo Alto Networks PAN-OS allows authenticated administrators to execute code with root privileges or delete arbitrary system files and impact the system's integrity or cause a denial of service condition. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14.	7.2	More Details
CVE-2020-2006	A stack-based buffer overflow vulnerability in the management server component of PAN-OS that allows an authenticated user to potentially execute arbitrary code with root privileges. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13129	An issue was discovered in the stashcat app through 3.9.1 for macOS, Windows, Android, iOS, and possibly other platforms. The GET method is used with client_key and device_id data in the query string, which allows attackers to obtain sensitive information by reading web-server logs.	7.2	More Details
CVE-2020-2007	An OS command injection vulnerability in the management server component of PAN-OS allows an authenticated user to potentially execute arbitrary commands with root privileges. This issue affects: All PAN-OS 7.1 versions; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	7.2	More Details
CVE-2020-2009	An external control of filename vulnerability in the SD WAN component of Palo Alto Networks PAN-OS Panorama allows an authenticated administrator to send a request that results in the creation and write of an arbitrary file on all firewalls managed by the Panorama. In some cases this results in arbitrary code execution with root permissions. This issue affects: All versions of PAN-OS 7.1; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.7.	7.2	More Details
CVE-2020-2005	A cross-site scripting (XSS) vulnerability exists when visiting malicious websites with the Palo Alto Networks GlobalProtect Clientless VPN that can compromise the user's active session. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.7; All versions of PAN-OS 8.0.	7.1	More Details
CVE-2020-4411	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service vulnerability in its kernel module that could allow an attacker to cause a denial of service condition on the affected system. To exploit this vulnerability, a local attacker could invoke a subset of ioctls on the Spectrum Scale device with non-valid arguments. This could allow the attacker to crash the kernel. IBM X-Force ID: 179986.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1808	Honor 20;HONOR 20 PRO;Honor Magic2;HUAWEI Mate 20 X;HUAWEI P30;HUAWEI P30 Pro;Honor View 20 smartphones with versions earlier than 10.0.0.187(C00E60R4P11); versions earlier than 10.0.0.187(C00E60R4P11); versions earlier than 10.0.0.176(C00E60R2P11);9.1.0.135(C00E133R2P1); versions earlier than 10.1.0.123(C431E22R3P5), versions earlier than 10.1.0.126(C636E5R3P4), versions earlier than 10.1.0.160(C00E160R2P11); versions earlier than 10.1.0.126(C185E8R5P1), versions earlier than 10.1.0.126(C636E9R2P4), versions earlier than 10.1.0.160(C00E160R2P8); versions earlier than 10.0.0.179(C636E3R4P3), versions earlier than 10.0.0.180(C185E3R3P3), versions earlier than 10.0.0.180(C432E10R3P4), versions earlier than 10.0.0.181(C675E5R1P2) have an out of bound read vulnerability. The software reads data past the end of the intended buffer. The attacker tricks the user into installing a crafted application, successful exploit may cause information disclosure or service abnormal.	7.1	More Details
CVE-2020-2016	A race condition due to insecure creation of a file in a temporary directory vulnerability in PAN-OS allows for root privilege escalation from a limited linux user account. This allows an attacker who has escaped the restricted shell as a low privilege administrator, possibly by exploiting another vulnerability, to escalate privileges to become root user. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; All versions of PAN-OS 8.0.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2004	Under certain circumstances a user's password may be logged in cleartext in the PanGPS.log diagnostic file when logs are collected for troubleshooting on GlobalProtect app (also known as GlobalProtect Agent) for MacOS and Windows. For this issue to occur all of these conditions must be true: (1) 'Save User Credential' option should be set to 'Yes' in the GlobalProtect Portal's Agent configuration, (2) the GlobalProtect user manually selects a gateway, (3) and the logging level is set to 'Dump' while collecting troubleshooting logs. This issue does not affect GlobalProtect app on other platforms (for example iOS/Android/Linux). This issue affects GlobalProtect app 5.0 versions earlier than 5.0.9, GlobalProtect app 5.1 versions earlier than 5.1.2 on Windows or MacOS. Since becoming aware of the issue, Palo Alto Networks has safely deleted all the known GlobalProtectLogs zip files sent by customers with the credentials. We now filter and remove these credentials from all files sent to Customer Support. The GlobalProtectLogs zip files uploaded to Palo Alto Networks systems were only accessible by authorized personnel with valid Palo Alto Networks credentials. We do not have any evidence of malicious access or use of these credentials.	6.8	More Details
CVE-2020-7137	A validation issue in HPE Superdome Flex's RMC component may allow local elevation of privilege. Apply HPE Superdome Flex Server version 3.25.46 or later to resolve this issue.	6.7	More Details
CVE-2020-0220	In crus_afe_callback of msm-cirrus-playback.c, there is a possible out of bounds write due to a missing bounds check. 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-139739561	6.7	More Details
CVE-2019-7246	An issue was discovered in atillk64.sys in AMD ATI Diagnostics Hardware Abstraction Sys/Overclocking Utility 5.11.9.0. The vulnerable driver exposes a wrmsr instruction and does not properly filter the Model Specific Register (MSR). Allowing arbitrary MSR writes can lead to Ring-0 code execution and escalation of privileges.	6.7	More Details
CVE-2020-11521	libfreerdp/codec/planar.c in FreeRDP version > 1.0 through 2.0.0-rc4 has an Out-of-bounds Write.	6.6	More Details
CVE-2020-11523	libfreerdp/gdi/region.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Integer Overflow.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11524	libfreerdp/codec/interleaved.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Out-of-bounds Write.	6.6	More Details
CVE-2019-13023	An issue was discovered in all versions of Bond JetSelect. Within the JetSelect Application, the web interface hides RADIUS secrets, WPA passwords, and SNMP strings from 'non administrative' users using HTML 'password field' obfuscation. By using Developer tools or similar, it is possible to change the obfuscation so that the credentials are visible.	6.5	More Details
CVE-2020-13154	Zoho ManageEngine Service Plus before 11.1 build 11112 allows low-privilege authenticated users to discover the File Protection password via a getFileProtectionSettings call to AjaxServlet.	6.5	More Details
CVE-2020-11522	libfreerdp/gdi/gdi.c in FreeRDP > 1.0 through 2.0.0-rc4 has an Out-of-bounds Read.	6.5	More Details
CVE-2020-11550	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK).	6.5	More Details
CVE-2020-2024	An improper link resolution vulnerability affects Kata Containers versions prior to 1.11.0. Upon container teardown, a malicious guest can trick the kata-runtime into unmounting any mount point on the host and all mount points underneath it, potentiality resulting in a host DoS.	6.5	More Details
CVE-2020-13143	gadget_dev_desc_UDC_store in drivers/usb/gadget/configfs.c in the Linux kernel 3.16 through 5.6.13 relies on kstrdup without considering the possibility of an internal '\0' value, which allows attackers to trigger an out-of-bounds read, aka CID-15753588bcd4.	6.5	More Details
CVE-2020-8020	A Improper Neutralization of Input During Web Page Generation vulnerability in open-build-service allows remote attackers to store arbitrary JS code to cause XSS. This issue affects: openSUSE open-build-service versions prior to 7cc32c8e2ff7290698e101d9a80a9dc29a5500fb.	6.5	More Details
CVE-2020-13135	D-Link DSP-W215 1.26b03 devices allow information disclosure by intercepting messages on the local network, as demonstrated by a Squid Proxy.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12717	The COVIDSafe (Australia) app 1.0 and 1.1 for iOS allows a remote attacker to crash the app, and consequently interfere with COVID-19 contact tracing, via a Bluetooth advertisement containing manufacturer data that is too short. This occurs because of an erroneous OpenTrace manuData.subdata call. The ABTraceTogether (Alberta), ProteGO (Poland), and TraceTogether (Singapore) apps were also affected.	6.5	More Details
CVE-2020-4286	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 176268.	6.5	More Details
CVE-2020-4259	IBM Sterling File Gateway 2.2.0.0 through 6.0.3.1 could allow an authenticated user could manipulate cookie information and remove or add modules from the cookie to access functionality not authorized to. IBM X-Force ID: 175638.	6.5	More Details
CVE-2019-13021	The administrative passwords for all versions of Bond JetSelect are stored within an unprotected file on the filesystem, rather than encrypted within the MySQL database. This backup copy of the passwords is made as part of the installation script, after the administrator has generated a password using ENCtool.jar (see CVE-2019-13022). This allows any low-privilege user who can read this file to trivially obtain the passwords for the administrative accounts of the JetSelect application. The path to the file containing the encoded password hash is /opt/JetSelect/SFC/resources/sfc-general-properties.	6.5	More Details
CVE-2020-12068	An issue was discovered in CODESYS Development System before 3.5.16.0. CODESYS WebVisu and CODESYS Remote TargetVisu are susceptible to privilege escalation.	6.5	More Details
CVE-2020-13125	An issue was discovered in the "Ultimate Addons for Elementor" plugin before 1.24.2 for WordPress, as exploited in the wild in May 2020 in conjunction with CVE-2020-13126. Unauthenticated attackers can create users with the Subscriber role even if registration is disabled.	6.5	More Details
CVE-2020-12042	Opto 22 SoftPAC Project Version 9.6 and prior. Paths specified within the zip files used to update the SoftPAC firmware are not sanitized. As a result, an attacker with user privileges can gain arbitrary file write access with system access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2003	An external control of filename vulnerability in the command processing of PAN-OS allows an authenticated administrator to delete arbitrary system files affecting the integrity of the system or causing denial of service to all PAN-OS services. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions before 8.1.14; PAN-OS 9.0 versions before 9.0.7; PAN-OS 9.1 versions before 9.1.1.	6.5	More Details
CVE-2020-5408	Spring Security versions 5.3.x prior to 5.3.2, 5.2.x prior to 5.2.4, 5.1.x prior to 5.1.10, 5.0.x prior to 5.0.16 and 4.2.x prior to 4.2.16 use a fixed null initialization vector with CBC Mode in the implementation of the queryable text encryptor. A malicious user with access to the data that has been encrypted using such an encryptor may be able to derive the unencrypted values using a dictionary attack.	6.5	More Details
CVE-2020-10134	Pairing in Bluetooth® Core v5.2 and earlier may permit an unauthenticated attacker to acquire credentials with two pairing devices via adjacent access when the unauthenticated user initiates different pairing methods in each peer device and an end-user erroneously completes both pairing procedures with the MITM using the confirmation number of one peer as the passkey of the other. An adjacent, unauthenticated attacker could be able to initiate any Bluetooth operation on either attacked device exposed by the enabled Bluetooth profiles. This exposure may be limited when the user must authorize certain access explicitly, but so long as a user assumes that it is the intended remote device requesting permissions, device-local protections may be weakened.	6.3	More Details
CVE-2020-12875	Veritas APTARE versions prior to 10.4 did not perform adequate authorization checks. An authenticated user could gain unauthorized access to sensitive information or functionality by manipulating specific parameters within the application.	6.3	More Details
CVE-2020-1945	Apache Ant 1.1 to 1.9.14 and 1.10.0 to 1.10.7 uses the default temporary directory identified by the Java system property java.io.tmpdir for several tasks and may thus leak sensitive information. The fixcrlf and replaceregexp tasks also copy files from the temporary directory back into the build tree allowing an attacker to inject modified source files into the build process.	6.3	More Details
CVE-2020-12699	The direct_mail extension through 5.2.3 for TYPO3 has an Open Redirect via jumpUrl.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13121	Submitty through 20.04.01 has an open redirect via authentication/login?old= during an invalid login attempt.	6.1	More Details
CVE-2020-12677	An issue was discovered in Progress MOVEit Automation Web Admin. A Web Admin application endpoint failed to adequately sanitize malicious input, which could allow an unauthenticated attacker to execute arbitrary code in a victim's browser, aka XSS. This affects 2018 - 2018.0 prior to 2018.0.3, 2018 SP1 - 2018.2 prior to 2018.2.3, 2018 SP2 - 2018.3 prior to 2018.3.7, 2019 - 2019.0 prior to 2019.0.3, 2019.1 - 2019.1 prior to 2019.1.2, and 2019.2 - 2019.2 prior to 2019.2.2.	6.1	More Details
CVE-2020-5409	Pivotal Concourse, most versions prior to 6.0.0, allows redirects to untrusted websites in its login flow. A remote unauthenticated attacker could convince a user to click on a link using the OAuth redirect link with an untrusted website and gain access to that user's access token in Concourse. (This issue is similar to, but distinct from, CVE-2018-15798.)	6.1	More Details
CVE-2020-13153	app/View/Events/resolved_attributes.ctp in MISP before 2.4.126 has XSS in the resolved attributes view.	6.1	More Details
CVE-2019-19456	A Reflected XSS was found in the server selection box inside the login page at: enginemanager/loginfailed.html in Wowza Streaming Engine <= 4.x.x. This issue was resolved in Wowza Streaming Engine 4.8.0.	6.1	More Details
CVE-2019-15083	Default installations of Zoho ManageEngine ServiceDesk Plus 10.0 before 10500 are vulnerable to XSS injected by a workstation local administrator. Using the installed program names of the computer as a vector, the local administrator can execute code on the Manage Engine ServiceDesk administrator side. At "Asset Home > Server > <workstation> > software" the administrator of ManageEngine can control what software is installed on the workstation. This table shows all the installed program names in the Software column. In this field, a remote attacker can inject malicious code in order to execute it when the ManageEngine administrator visualizes this page.	6.1	More Details
CVE-2019-20802	An issue was discovered in the Readdle Documents app before 6.9.7 for iOS. The application's file-transfer web server improperly displays directory names, leading to Stored XSS, which may be used to steal a user's data. This requires user interaction because there is no known direct way for an attacker to create a crafted directory name on a victim's device. However, a crafted directory name can occur if a victim extracts a ZIP archive that was provided by an attacker.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12685	XSS in the admin help system admin/help.html and admin/quicklinks.html in Interchange 4.7.0 through 5.11.x allows remote attackers to steal credentials or data via browser JavaScript.	6.1	More Details
CVE-2020-1941	In Apache ActiveMQ 5.0.0 to 5.15.11, the webconsole admin GUI is open to XSS, in the view that lists the contents of a queue.	6.1	More Details
CVE-2020-6956	PCS DEXICON 3.4.1 allows XSS via the loginName parameter in login_action.jsp.	6.1	More Details
CVE-2020-8035	The image view functionality in Horde Groupware Webmail Edition before 5.2.22 is affected by a stored Cross-Site Scripting (XSS) vulnerability via an SVG image upload containing a JavaScript payload. An attacker can obtain access to a victim's webmail account by making them visit a malicious URL.	6.1	More Details
CVE-2020-12742	The iubenda-cookie-law-solution plugin before 2.3.5 for WordPress does not restrict URL sanitization to http protocols.	6.1	More Details
CVE-2020-5575	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4606 (7.2.1) and earlier (Movable Type 7), Movable Type Advanced 7 r.4606 (7.2.1) and earlier (Movable Type Advanced 7), Movable Type for AWS 7 r.4606 (7.2.1) and earlier (Movable Type for AWS 7), Movable Type 6.5.3 and earlier (Movable Type 6.5), Movable Type Advanced 6.5.3 and earlier (Movable Type Advanced 6.5), Movable Type 6.3.11 and earlier (Movable Type 6.3), Movable Type Advanced 6.3.11 and earlier (Movable Type 6.3), Movable Type Premium 1.29 and earlier, and Movable Type Premium Advanced 1.29 and earlier) allows remote attackers to inject arbitrary script or HTML via unspecified vectors.	6.1	More Details
CVE-2020-11845	Cross Site Scripting vulnerability in Micro Focus Service Manager product. Affecting versions 9.50, 9.51, 9.52, 9.60, 9.61, 9.62, 9.63. The vulnerability could be exploited to allow remote attackers to inject arbitrary web script or HTML.	6.1	More Details
CVE-2019-20389	An XSS issue was identified on the Subrion CMS 4.2.1 /panel/configuration/general settings page. A remote attacker can inject arbitrary JavaScript code in the v[language_switch] parameter (within multipart/form-data), which is reflected back within a user's browser without proper output encoding.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8034	Gollem before 3.0.13, as used in Horde Groupware Webmail Edition 5.2.22 and other products, is affected by a reflected Cross-Site Scripting (XSS) vulnerability via the HTTP GET dir parameter in the browser functionality, affecting breadcrumb output. An attacker can obtain access to a victim's webmail account by making them visit a malicious URL.	6.1	More Details
CVE-2020-7656	jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.	6.1	More Details
CVE-2019-2388	In affected Ops Manager versions there is an exposed http route was that may allow attackers to view a specific access log of a publicly exposed Ops Manager instance. This issue affects: MongoDB Inc. MongoDB Ops Manager 4.0 versions 4.0.9, 4.0.10 and MongoDB Ops Manager 4.1 version 4.1.5.	5.8	More Details
CVE-2020-12046	Opto 22 SoftPAC Project Version 9.6 and prior. SoftPAC's firmware files' signatures are not verified upon firmware update. This allows an attacker to replace legitimate firmware files with malicious files.	5.7	More Details
CVE-2020-0065	An improper authorization in the receiver component of the Android Suite Daemon.Product: AndroidVersions: Android SoCAndroid ID: A-149813448	5.5	More Details
CVE-2020-6093	An exploitable information disclosure vulnerability exists in the way Nitro Pro 13.9.1.155 does XML error handling. A specially crafted PDF document can cause uninitialized memory access resulting in information disclosure. In order to trigger this vulnerability, victim must open a malicious file.	5.5	More Details
CVE-2020-9501	Attackers can obtain Cloud Key information from the Dahua Web P2P control in specific ways. Cloud Key is used to authenticate the connection between the client tool and the platform. An attacker may use the leaked Cloud Key to impersonate the client to connect to the platform, resulting in additional consumption of platform server resources. Versions with Build time before April 2020 are affected.	5.5	More Details
CVE-2020-3810	Missing input validation in the ar/tar implementations of APT before version 2.1.2 could result in denial of service when processing specially crafted deb files.	5.5	More Details
CVE-2020-0064	An improper authorization while processing the provisioning data.Product: AndroidVersions: Android SoCAndroid ID: A-149866855	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0091	In mnld, an incorrect configuration in driver_cfg of mnld for meta factory mode.Product: AndroidVersions: Android SoCAndroid ID: A-149808700	5.5	More Details
CVE-2020-0090	An improper authorization in the receiver component of Email.Product: AndroidVersions: Android SoCAndroid ID: A-149813048	5.5	More Details
CVE-2020-12038	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable. A memory corruption vulnerability exists in the algorithm that matches square brackets in the EDS subsystem. This may allow an attacker to craft specialized EDS files to crash the EDSParser COM object, leading to denial-of-service conditions.	5.5	More Details
CVE-2020-12872	yaws_config.erl in Yaws through 2.0.2 and/or 2.0.7 loads obsolete TLS ciphers, as demonstrated by ones that allow Sweet32 attacks, if running on an Erlang/OTP virtual machine with a version less than 21.0.	5.5	More Details
CVE-2020-0100	In onTransact of IHDCP.cpp, there is a possible out of bounds read due to incorrect error handling. This could lead to local information disclosure of data from a privileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-8.0Android ID: A-150156584	5.5	More Details
CVE-2020-0101	In BnCrypto::onTransact of ICrypto.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144767096	5.5	More Details
CVE-2020-0104	In onShowingStateChanged of KeyguardStateMonitor.java, there is a possible inappropriate read due to a logic error. This could lead to local information disclosure of keyguard-protected data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144430870	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0106	In getCellLocation of PhoneInterfaceManager.java, there is a possible permission bypass due to a missing SDK version check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148414207	5.5	More Details
CVE-2020-7455	In FreeBSD 12.1-STABLE before r360973, 12.1-RELEASE before p5, 11.4-STABLE before r360973, 11.4-BETA1 before p1 and 11.3-RELEASE before p9, the FTP packet handler in libalias incorrectly calculates some packet length allowing disclosure of small amounts of kernel (for kernel NAT) or natd process space (for userspace natd).	5.5	More Details
CVE-2020-13094	Dolibarr before 11.0.4 allows XSS.	5.4	More Details
CVE-2020-13145	Studio in Open edX Ironwood 2.5 allows users to upload SVG files via the "Content>File Uploads" screen. These files can contain JavaScript code and thus lead to Stored XSS.	5.4	More Details
CVE-2020-12256	rConfig 3.9.4 is vulnerable to reflected XSS. The devicemgmnt.php file improperly validates user input. An attacker can exploit this by crafting arbitrary JavaScript in the deviceId GET parameter to devicemgmnt.php.	5.4	More Details
CVE-2020-11065	In TYPO3 CMS greater than or equal to 9.5.12 and less than 9.5.17, and greater than or equal to 10.2.0 and less than 10.4.2, it has been discovered that link tags generated by typolink functionality are vulnerable to cross-site scripting; properties being assigned as HTML attributes have not been parsed correctly. This has been fixed in 9.5.17 and 10.4.2.	5.4	More Details
CVE-2020-9524	Cross Site scripting vulnerability on Micro Focus Enterprise Server and Enterprise developer, affecting all versions prior to version 5.0 Patch Update 8. The vulnerability could allow an attacker to trigger administrative actions when an administrator viewed malicious data left by the attacker (stored XSS) or followed a malicious link (reflected XSS).	5.4	More Details
CVE-2020-11070	The SVG Sanitizer extension for TYPO3 has a cross-site scripting vulnerability in versions before 1.0.3. Slightly invalid or incomplete SVG markup is not correctly processed and thus not sanitized at all. Albeit the markup is not valid it still is evaluated in browsers and leads to cross-site scripting. This is fixed in version 1.0.3.	5.4	More Details
CVE-2020-12259	rConfig 3.9.4 is vulnerable to reflected XSS. The configDevice.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the rid GET parameter of devicemgmnt.php.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4298	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176475.	5.4	More Details
CVE-2020-11064	In TYPO3 CMS greater than or equal to 9.0.0 and less than 9.5.17 and greater than or equal to 10.0.0 and less than 10.4.2, it has been discovered that HTML placeholder attributes containing data of other database records are vulnerable to cross-site scripting. A valid backend user account is needed to exploit this vulnerability. This has been fixed in 9.5.17 and 10.4.2.	5.4	More Details
CVE-2020-10135	Legacy pairing and secure-connections pairing authentication in Bluetooth BR/EDR Core Specification v5.2 and earlier may allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. An unauthenticated, adjacent attacker could impersonate a Bluetooth BR/EDR master or slave to pair with a previously paired remote device to successfully complete the authentication procedure without knowing the link key.	5.4	More Details
CVE-2020-1998	An improper authorization vulnerability in PAN-OS that mistakenly uses the permissions of local linux users instead of the intended SAML permissions of the account when the username is shared for the purposes of SSO authentication. This can result in authentication bypass and unintended resource access for the user. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; PAN-OS 9.1 versions earlier than 9.1.1; All versions of PAN-OS 8.0.	5.4	More Details
CVE-2020-12882	Submitty through 20.04.01 allows XSS via upload of an SVG document, as demonstrated by an attack by a Student against a Teaching Fellow.	5.4	More Details
CVE-2020-5574	HTML attribute value injection vulnerability in Movable Type series (Movable Type 7 r.4606 (7.2.1) and earlier (Movable Type 7), Movable Type Advanced 7 r.4606 (7.2.1) and earlier (Movable Type Advanced 7), Movable Type for AWS 7 r.4606 (7.2.1) and earlier (Movable Type for AWS 7), Movable Type 6.5.3 and earlier (Movable Type 6.5), Movable Type Advanced 6.5.3 and earlier (Movable Type Advanced 6.5), Movable Type 6.3.11 and earlier (Movable Type 6.3), Movable Type Advanced 6.3.11 and earlier (Movable Type 6.3), Movable Type Premium 1.29 and earlier, and Movable Type Premium Advanced 1.29 and earlier) allows remote attackers to inject arbitrary HTML attribute value via unspecified vectors.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4412	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service security vulnerability. An attacker can force the Spectrum Scale mmfsd/mmsdrserv daemons to unexpectedly exit, impacting the functionality of the Spectrum Scale cluster and the availability of file systems managed by Spectrum Scale. IBM X-Force ID: 179987.	5.3	More Details
CVE-2020-12697	The direct_mail extension through 5.2.3 for TYPO3 allows Denial of Service via log entries.	5.3	More Details
CVE-2020-8021	a Improper Access Control vulnerability in of Open Build Service allows remote attackers to read files of an OBS package where the sourceaccess/access is disabled This issue affects: Open Build Service versions prior to 2.10.5.	5.3	More Details
CVE-2020-12860	COVIDSafe through v1.0.17 allows a remote attacker to access phone name and model information because a BLE device can have four roles and COVIDSafe uses all of them. This allows for re-identification of a device, and potentially identification of the owner's name.	5.3	More Details
CVE-2020-12859	Unnecessary fields in the OpenTrace/BlueTrace protocol in COVIDSafe through v1.0.17 allow a remote attacker to identify a device model by observing cleartext payload data. This allows re-identification of devices, especially less common phone models or those in low-density situations.	5.3	More Details
CVE-2020-10958	In Dovecot before 2.3.10.1, a crafted SMTP/LMTP message triggers an unauthenticated use-after-free bug in submission-login, submission, or lmtp, and can lead to a crash under circumstances involving many newlines after a command.	5.3	More Details
CVE-2020-12888	The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory space.	5.3	More Details
CVE-2020-13093	iSpyConnect.com Agent DVR before 2.7.1.0 allows directory traversal.	5.3	More Details
CVE-2020-1758	A flaw was found in Keycloak in versions before 10.0.0, where it does not perform the TLS hostname verification while sending emails using the SMTP server. This flaw allows an attacker to perform a man-in-the-middle (MITM) attack.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-17572	In Apache RocketMQ 4.2.0 to 4.6.0, when the automatic topic creation in the broker is turned on by default, an evil topic like “../../../../topic2020” is sent from rocketmq-client to the broker, a topic folder will be created in the parent directory in brokers, which leads to a directory traversal vulnerability. Users of the affected versions should apply one of the following: Upgrade to Apache RocketMQ 4.6.1 or later.	5.3	More Details
CVE-2019-20801	An issue was discovered in the Readdle Documents app before 6.9.7 for iOS. The application's file-transfer web server allows for cross-origin requests from any domain, and the WebSocket server lacks authorization control. Any web site can execute JavaScript code (that accesses a user's data) via cross-origin requests.	5.3	More Details
CVE-2020-1996	A missing authorization vulnerability in the management server component of PAN-OS Panorama allows a remote unauthenticated user to inject messages into the management server ms.log file. This vulnerability can be leveraged to obfuscate an ongoing attack or fabricate log entries in the ms.log file This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.9.	5.3	More Details
CVE-2020-1997	An open redirection vulnerability in the GlobalProtect component of Palo Alto Networks PAN-OS allows an attacker to specify an arbitrary redirection target away from the trusted GlobalProtect gateway. If the user then successfully authenticates it will cause them to access an unexpected and potentially malicious website. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.0 versions earlier than 8.0.14.	5.3	More Details
CVE-2020-10967	In Dovecot before 2.3.10.1, remote unauthenticated attackers can crash the lmtp or submission process by sending mail with an empty localpart.	5.3	More Details
CVE-2020-12831	An issue was discovered in FRRouting FRR (aka Free Range Routing) through 7.3.1. When using the split-config feature, the init script creates an empty config file with world-readable default permissions, leading to a possible information leak via tools/frr.in and tools/frrcommon.sh.in. NOTE: some parties consider this user error, not a vulnerability, because the permissions are under the control of the user before any sensitive information is present in the file	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12801	If LibreOffice has an encrypted document open and crashes, that document is auto-saved encrypted. On restart, LibreOffice offers to restore the document and prompts for the password to decrypt it. If the recovery is successful, and if the file format of the recovered document was not LibreOffice's default ODF file format, then affected versions of LibreOffice default that subsequent saves of the document are unencrypted. This may lead to a user accidentally saving a MSOffice file format document unencrypted while believing it to be encrypted. This issue affects: LibreOffice 6-3 series versions prior to 6.3.6; 6-4 series versions prior to 6.4.3.	5.3	More Details
CVE-2020-10724	A vulnerability was found in DPDK versions 18.11 and above. The vhost-crypto library code is missing validations for user-supplied values, potentially allowing an information leak through an out-of-bounds memory read.	5.1	More Details
CVE-2020-10723	A memory corruption issue was found in DPDK versions 17.05 and above. This flaw is caused by an integer truncation on the index of a payload. Under certain circumstances, the index (a UInt) is copied and truncated into a uint16, which can lead to out of bound indexing and possible memory corruption.	5.1	More Details
CVE-2020-10722	A vulnerability was found in DPDK versions 18.05 and above. A missing check for an integer overflow in vhost_user_set_log_base() could result in a smaller memory map than requested, possibly allowing memory corruption.	5.1	More Details
CVE-2020-10744	An incomplete fix was found for the fix of the flaw CVE-2020-1733 ansible: insecure temporary directory when running become_user from become directive. The provided fix is insufficient to prevent the race condition on systems using ACLs and FUSE filesystems. Ansible Engine 2.7.18, 2.8.12, and 2.9.9 as well as previous versions are affected and Ansible Tower 3.4.5, 3.5.6 and 3.6.4 as well as previous versions are affected.	5.0	More Details
CVE-2020-0093	In exif_data_save_data_entry of exif-data.c, 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-8.0 Android-8.1 Android-9 Android-10Android ID: A-148705132	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-0092	In setHideSensitive of NotificationStackScrollLayout.java, there is a possible disclosure of sensitive notification content due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145135488	5.0	More Details
CVE-2020-1995	A NULL pointer dereference vulnerability in Palo Alto Networks PAN-OS allows an authenticated administrator to send a request that causes the rasmgr daemon to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue affects: PAN-OS 9.1 versions earlier than 9.1.2.	4.9	More Details
CVE-2020-5838	Symantec IT Analytics, prior to 2.9.1, may be susceptible to a cross-site scripting (XSS) exploit, which is a type of issue that can potentially enable attackers to inject client-side scripts into web pages viewed by other users.	4.8	More Details
CVE-2020-1960	A vulnerability in Apache Flink (1.1.0 to 1.1.5, 1.2.0 to 1.2.1, 1.3.0 to 1.3.3, 1.4.0 to 1.4.2, 1.5.0 to 1.5.6, 1.6.0 to 1.6.4, 1.7.0 to 1.7.2, 1.8.0 to 1.8.3, 1.9.0 to 1.9.2, 1.10.0) where, when running a process with an enabled JMXReporter, with a port configured via metrics.reporter.reporter_name>.port, an attacker with local access to the machine and JMX port can execute a man-in-the-middle attack using a specially crafted request to rebind the JMXRMI registry to one under the attacker's control. This compromises any connection established to the process via JMX, allowing extraction of credentials and any other transferred data.	4.7	More Details
CVE-2020-7809	ALSong 3.46 and earlier version contain a Document Object Model (DOM) based cross-site scripting vulnerability caused by improper validation of user input. A remote attacker could exploit this vulnerability by tricking the victim to open ALSong Album(sab) file.	4.4	More Details
CVE-2020-12698	The direct_mail extension through 5.2.3 for TYPO3 has Broken Access Control for newsletter subscriber tables.	4.3	More Details
CVE-2020-4365	IBM WebSphere Application Server 8.5 is vulnerable to server-side request forgery. By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 178964.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4299	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.1 could expose sensitive information to a user through a specially crafted HTTP request. IBM X-Force ID: 176606.	4.3	More Details
CVE-2020-4312	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 trough 6.0.3.1 could allow an authenticated user to obtain sensitive information from a cached web page. IBM X-Force ID: 177089.	4.3	More Details
CVE-2020-12700	The direct_mail extension through 5.2.3 for TYPO3 allows Information Disclosure via a newsletter subscriber data Special Query.	4.3	More Details
CVE-2020-1994	A predictable temporary file vulnerability in PAN-OS allows a local authenticated user with shell access to corrupt arbitrary system files affecting the integrity of the system. This issue affects: All versions of PAN-OS 7.1 and 8.0; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.7.	4.1	More Details
CVE-2020-1993	The GlobalProtect Portal feature in PAN-OS does not set a new session identifier after a successful user login, which allows session fixation attacks, if an attacker is able to control a user's session ID. This issue affects: All PAN-OS 7.1 and 8.0 versions; PAN-OS 8.1 versions earlier than 8.1.14; PAN-OS 9.0 versions earlier than 9.0.8.	3.7	More Details
CVE-2020-11063	In TYPO3 CMS versions 10.4.0 and 10.4.1, it has been discovered that time-based attacks can be used with the password reset functionality for backend users. This allows an attacker to mount user enumeration based on email addresses assigned to backend user accounts. This has been fixed in 10.4.2.	3.7	More Details
CVE-2020-4345	IBM i 7.2, 7.3, and 7.4 users running complex SQL statements under a specific set of circumstances may allow a local user to obtain sensitive information that they should not have access to. IBM X-Force ID: 178318.	3.3	More Details
CVE-2020-11931	An Ubuntu-specific modification to Pulseaudio to provide security mediation for Snap-packaged applications was found to have a bypass of intended access restriction for snaps which plugs any of pulseaudio, audio-playback or audio-record via unloading the pulseaudio snap policy module. This issue affects: pulseaudio 1:8.0 versions prior to 1:8.0-0ubuntu3.12; 1:11.1 versions prior to 1:11.1-1ubuntu7.7; 1:13.0 versions prior to 1:13.0-1ubuntu1.2; 1:13.99.1 versions prior to 1:13.99.1-1ubuntu3.2;	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9073	Huawei P20 smartphones with versions earlier than 10.0.0.156(C00E156R1P4) have an improper authentication vulnerability. The vulnerability is due to that when an user wants to do certain operation, the software insufficiently validate the user's identity. Attackers need to physically access the smartphone to exploit this vulnerability. Successful exploit could allow the attacker to bypass the limit of student mode function.	2.4	More Details
CVE-2020-11932	It was discovered that the Subiquity installer for Ubuntu Server logged the LUKS full disk encryption password if one was entered.	2.3	More Details
CVE-2020-11525	libfreerdp/cache/bitmap.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Out of bounds read.	2.2	More Details
CVE-2020-11526	libfreerdp/core/update.c in FreeRDP versions > 1.1 through 2.0.0-rc4 has an Out-of-bounds Read.	2.2	More Details
CVE-2020-12440	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