SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 July 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 Number	Description	Base Score	Reference
CVE-2020-2021	When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability. This issue affects PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL). This issue does not affect PAN-OS 7.1. This issue cannot be exploited if SAML is not used for authentication. This issue cannot be exploited if the 'Validate Identity Provider Certificate' option is enabled (checked) in the SAML Identity Provider Server Profile. Resources that can be protected by SAML-based single sign-on (SSO) authentication are: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN, Authentication and Captive Portal, PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces, Prisma Access In the case of GlobalProtect Gateways, GlobalProtect Portal, Clientless VPN, Captive Portal, and Prisma Access, an unauthenticated attacker with network access to the affected servers can gain access to protected resources if allowed by configured authentication and Security policies. There is no impact on the integrity and availability of the gateway, portal or VPN server. An attacker cannot inspect or tamper with sessions of regular users. In the worst case, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N). In the case of PAN-OS and Panorama web interfaces, this issue allows an unauthenticated attacker with network access to the PAN-OS or Panorama web interfaces to log in as an administrator and perform administrative actions. In the worst-case scenario, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). If the web interfaces are only accessible to a restricted management network, then the issue is lowered to a CVSS Base Score of 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). Palo Alto Networks is not aware of any malicious attempts to exploit this vulnerability.	10.0	More Details
CVE-2018-21268	The traceroute (aka node-traceroute) package through 1.0.0 for Node.js allows remote command injection via the host parameter. This occurs because the Child.exec() method, which is considered to be not entirely safe, is used. In particular, an OS command can be placed after a newline character.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15049	An issue was discovered in http/ContentLengthInterpreter.cc in Squid before 4.12 and 5.x before 5.0.3. A Request Smuggling and Poisoning attack can succeed against the HTTP cache. The client sends an HTTP request with a Content-Length header containing "+\ "-" or an uncommon shell whitespace character prefix to the length field-value.	9.9	More Details
CVE-2020-15323	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the cloud1234 password for the a1@chopin account default credentials.	9.8	More Details
CVE-2020-12016	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 have hard-coded administrative account credentials for the ExactaMix operating system. Successful exploitation of this vulnerability may allow an attacker who has gained unauthorized access to system resources, including access to execute software or to view/update files, directories, or system configuration. This could allow an attacker with network access to view sensitive data including PHI.	9.8	More Details
CVE-2020-12040	Sigma Spectrum Infusion System v's6.x (model 35700BAX) and Baxter Spectrum Infusion System Version(s) 8.x (model 35700BAX2) at the application layer uses an unauthenticated clear-text communication channel to send and receive system status and operational data. This could allow an attacker that has circumvented network security measures to view sensitive non-private data or to perform a man-in-the-middle attack.	9.8	More Details
CVE-2020-12043	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when configured for wireless networking the FTP service operating on the WBM remains operational until the WBM is rebooted.	9.8	More Details
CVE-2020-12045	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when used in conjunction with a Baxter Spectrum v8.x (model 35700BAX2), operates a Telnet service on Port 1023 with hard-coded credentials.	9.8	More Details
CVE-2020-12047	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24), when used with a Baxter Spectrum v8.x (model 35700BAX2) in a factory-default wireless configuration enables an FTP service with hard-coded credentials.	9.8	More Details
CVE-2020-15320	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the axiros password for the root account.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15321	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the axzyxel password for the livedbuser account.	9.8	More Details
CVE-2020-15322	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the wbboEZ4BN3ssxAfM hardcoded password for the debian-sys-maint account.	9.8	More Details
CVE-2020-15324	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a world-readable axess/opt/axXMPPHandler/config/xmpp_config.py file that stores hardcoded credentials.	9.8	More Details
CVE-2020-10270	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000.	9.8	More Details
CVE-2020-14068	An issue was discovered in MK-AUTH 19.01. The web login functionality allows an attacker to bypass authentication and gain client privileges via SQL injection in central/executar_login.php.	9.8	More Details
CVE-2020-14070	An issue was discovered in MK-AUTH 19.01. There is authentication bypass in the web login functionality because guessable credentials to admin/executar_login.php result in admin access.	9.8	More Details
CVE-2020-14072	An issue was discovered in MK-AUTH 19.01. It allows command execution as root via shell metacharacters to /auth admin scripts.	9.8	More Details
CVE-2020-15362	wifiscanner.js in thingsSDK WiFi Scanner 1.0.1 allows Code Injection because it can be used with options to overwrite the default executable/binary path and its arguments. An attacker can abuse this functionality to execute arbitrary code.	9.8	More Details
CVE-2018-6446	A vulnerability in Brocade Network Advisor Version Before 14.3.1 could allow an unauthenticated, remote attacker to log in to the JBoss Administration interface of an affected system using an undocumented user credentials and install additional JEE applications.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15069	Sophos XG Firewall 17.x through v17.5 MR12 allows a Buffer Overflow and remote code execution via the HTTP/S Bookmarks feature for clientless access. Hotfix HF062020.1 was published for all firewalls running v17.x.	9.8	More Details
CVE-2017-18922	It was discovered that websockets.c in LibVNCServer prior to 0.9.12 did not properly decode certain WebSocket frames. A malicious attacker could exploit this by sending specially crafted WebSocket frames to a server, causing a heap-based buffer overflow.	9.8	More Details
CVE-2019-20893	An issue was discovered in Activision Infinity Ward Call of Duty Modern Warfare 2 through 2019-12-11. PartyHost_HandleJoinPartyRequest has a buffer overflow vulnerability and can be exploited by using a crafted joinParty packet. This can be utilized to conduct arbitrary code execution on a victim's machine.	9.8	More Details
CVE-2020-15411	An issue was discovered in MISP 2.4.128. app/Controller/AttributesController.php has insufficient ACL checks in the attachment downloader.	9.8	More Details
CVE-2020-15415	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472.	9.8	More Details
CVE-2020-15363	The Nexos theme through 1.7 for WordPress allows side-map/?search_order= SQL Injection.	9.8	More Details
CVE-2020-10269	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000.	9.8	More Details
CVE-2020-9631	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9630	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a business logic error vulnerability. Successful exploitation could lead to privilege escalation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10271	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS).	9.8	More Details
CVE-2020-10272	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire.	9.8	More Details
CVE-2020-10275	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data.	9.8	More Details
CVE-2020-10276	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device.	9.8	More Details
CVE-2020-10279	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks.	9.8	More Details
CVE-2020-15007	A buffer overflow in the M_LoadDefaults function in m_misc.c in id Tech 1 (aka Doom engine) allows arbitrary code execution via an unsafe usage of fscanf, because it does not limit the number of characters to be read in a format argument.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13484	Bitrix24 through 20.0.975 allows SSRF via an intranet IP address in the services/main/ajax.php?action=attachUrlPreview url parameter, if the destination URL hosts an HTML document containing '<meta name="og:image" content="' followed by an intranet URL.	9.8	More Details
CVE-2020-14094	In Xiaomi router R3600, ROM version<1.0.20, the connection service can be injected through the web interface, resulting in stack overflow or remote code execution.	9.8	More Details
CVE-2020-14095	In Xiaomi router R3600, ROM version<1.0.20, a connect service suffers from an injection vulnerability through the web interface, leading to a stack overflow or remote code execution.	9.8	More Details
CVE-2020-10561	An issue was discovered on Xiaomi Mi Jia ink-jet printer < 3.4.6_0138. Injecting parameters to ippserver through the web management background, resulting in command execution vulnerabilities.	9.8	More Details
CVE-2020-11960	Xiaomi router R3600 ROM before 1.0.50 is affected by a vulnerability when checking backup file in c_upload interface let attacker able to extract malicious file under any location in /tmp, lead to possible RCE and DoS	9.8	More Details
CVE-2020-14472	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file.	9.8	More Details
CVE-2020-14473	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B with firmware before 1.5.1.1.	9.8	More Details
CVE-2020-15348	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 allows use of live/CPEManager/AXCampaignManager/delete_cpes_by_ids?cpe_ids= for eval injection of Python code.	9.8	More Details
CVE-2020-9576	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9578	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9579	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9580	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9582	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9583	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9585	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-9632	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-12041	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) telnet Command-Line Interface, grants access to sensitive data stored on the WBM that permits temporary configuration changes to network settings of the WBM, and allows the WBM to be rebooted. Temporary configuration changes to network settings are removed upon reboot.	9.4	More Details
CVE-2020-12032	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view or modify sensitive data including PHI.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2020-14412	NeDi 1.9C is vulnerable to Remote Command Execution. System-Snapshot.php improperly escapes shell metacharacters from a POST request. An attacker can exploit this by crafting an arbitrary payload (any system commands) that contains shell metacharacters via a POST request with a psw parameter. (This can also be exploited via CSRF.)	8.8	More Details
CVE-2020-14947	OCS Inventory NG 2.7 allows Remote Command Execution via shell metacharacters to require/commandLine/CommandLine.php because mib_file in plugins/main_sections/ms_config/ms_snmp_config.php is mishandled in get_mib_oid.	8.8	More Details
CVE-2020-15046	The web interface on Supermicro X10DRH-iT motherboards with BIOS 2.0a and IPMI firmware 03.40 allows remote attackers to exploit a cgi/config_user.cgi CSRF issue to add new admin users. The fixed versions are BIOS 3.2 and firmware 03.88.	8.8	More Details
CVE-2020-13095	Little Snitch version 4.5.1 and older changed ownership of a directory path controlled by the user. This allowed the user to escalate to root by linking the path to a directory containing code executed by root.	8.8	More Details
CVE-2020-5601	Chrome Extension for e-Tax Reception System Ver1.0.0.0 allows remote attackers to execute an arbitrary command via unspecified vectors.	8.8	More Details
CVE-2019-16213	Tenda PA6 Wi-Fi Powerline extender 1.0.1.21 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted string, an attacker could modify the device name of an attached PLC adapter to inject and execute arbitrary commands on the system with root privileges.	8.8	More Details
CVE-2020-13443	ExpressionEngine before 5.3.2 allows remote attackers to upload and execute arbitrary code in a .php%20 file via Compose Msg, Add attachment, and Save As Draft actions. A user with low privileges (member) is able to upload this. It is possible to bypass the MIME type check and file-extension check while uploading new files. Short aliases are not used for an attachment; instead, direct access is allowed to the uploaded files. It is possible to upload PHP only if one has member access, or registration/forum is enabled and one can create a member with the default group id of 5. To exploit this, one must to be able to send and compose messages (at least).	8.8	More Details
CVE-2020-14414	NeDi 1.9C is vulnerable to Remote Command Execution. pwsec.php improperly escapes shell metacharacters from a POST request. An attacker can exploit this by crafting an arbitrary payload (any system commands) that contains shell metacharacters via a POST request with a pw parameter. (This can also be exploited via CSRF.)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14005	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows remote attackers to execute arbitrary code via a defined event.	8.8	More Details
CVE-2020-9414	The MFT admin service component of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contains a vulnerability that theoretically allows an authenticated user with specific permissions to obtain the session identifier of another user. The session identifier when replayed could provide administrative rights or file transfer permissions to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below.	8.8	More Details
CVE-2020-15014	pramodmahato BlogCMS through 2019-12-31 has admin/changepass.php CSRF.	8.8	More Details
CVE-2019-19505	Tenda PA6 Wi-Fi Powerline extender 1.0.1.21 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking by the "Wireless" section in the web-UI. By sending a specially crafted hostname, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the application to crash.	8.8	More Details
CVE-2020-9612	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-9597	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-12861	A heap buffer overflow in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to execute arbitrary code, aka GHSL-2020-080.	8.8	More Details
CVE-2020-3962	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a use-after-free vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3968	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds write vulnerability in the USB 3.0 controller (xHCI). A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to crash the virtual machine's vmx process leading to a denial of service condition or execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible.	8.2	More Details
CVE-2020-5580	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to view and/or alter Single sign-on settings via unspecified vectors.	8.1	More Details
CVE-2020-11538	In libImaging/SgiRleDecode.c in Pillow through 7.0.0, a number of out-of-bounds reads exist in the parsing of SGI image files, a different issue than CVE-2020-5311.	8.1	More Details
CVE-2020-6870	The version V12.17.20T115 of ZTE U31R20 product is impacted by a design error vulnerability. An attacker could exploit the vulnerability to log in to the FTP server to tamper with the password, and illegally download, modify, upload, or delete files, causing improper operation of the network management system and equipment. This affects: NetNumenU31R20 V12.17.20T115	8.0	More Details
CVE-2020-12865	A heap buffer overflow in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to execute arbitrary code, aka GHSL-2020-084.	8.0	More Details
CVE-2020-9637	Adobe After Effects versions 17.1 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9638	Adobe After Effects versions 17.1 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9606	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9661	Adobe After Effects versions 17.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9660	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9659	Adobe Audition versions 13.0.6 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9658	Adobe Audition versions 13.0.6 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9657	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-15397	HylaFAX+ through 7.0.2 and HylaFAX Enterprise have scripts that execute binaries from directories writable by unprivileged users (e.g., locations under /var/spool/hylafax that are writable by the uucp account). This allows these users to execute code in the context of the user calling these binaries (often root).	7.8	More Details
CVE-2020-9607	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9656	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-15395	In MediaInfoLib in MediaArea MediaInfo 20.03, there is a stack-based buffer over-read in Streams_Fill_PerStream in Multiple/File_MpegPs.cpp (aka an off-by-one during MpegPs parsing).	7.8	More Details
CVE-2020-9655	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9575	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-15396	In HylaFAX+ through 7.0.2 and HylaFAX Enterprise, the faxsetup utility calls chown on files in user-owned directories. By winning a race, a local attacker could use this to escalate his privileges to root.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9594	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9654	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9653	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9652	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9642	Adobe Illustrator versions 24.1.2 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9592	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	7.8	More Details
CVE-2020-10379	In Pillow before 7.1.0, there are two Buffer Overflows in libImaging/TiffDecode.c.	7.8	More Details
CVE-2020-9641	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-5966	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges.	7.8	More Details
CVE-2020-9613	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9596	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	7.8	More Details
CVE-2020-5964	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure.	7.8	More Details
CVE-2020-9640	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9639	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-14956	In Windows cleaning assistant 3.2, the driver file (AtpKrnl.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x223CCA.	7.8	More Details
CVE-2020-9614	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	7.8	More Details
CVE-2020-5963	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure.	7.8	More Details
CVE-2020-14957	In Windows cleaning assistant 3.2, the driver file (AtpKrnl.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x223CCD.	7.8	More Details
CVE-2020-9563	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9564	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9565	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9566	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9567	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9568	Adobe Bridge versions 10.0.1 and earlier version have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9569	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9570	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9571	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-5968	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which the software does not restrict or incorrectly restricts operations within the boundaries of a resource that is accessed by using an index or pointer, such as memory or files, which may lead to code execution, denial of service, escalation of privileges, or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	7.8	More Details
CVE-2020-9572	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9573	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9574	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5971	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which the software reads from a buffer by using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer, which may lead to code execution, denial of service, escalation of privileges, or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	7.8	More Details
CVE-2020-15360	com.docker.vmnetd in Docker Desktop 2.3.0.3 allows privilege escalation because of a lack of client verification.	7.8	More Details
CVE-2020-9562	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9561	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9560	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9620	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9662	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-5962	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges.	7.8	More Details
CVE-2020-9604	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15351	IDrive before 6.7.3.19 on Windows installs by default to %PROGRAMFILES(X86)%\IDriveWindows with weak folder permissions granting any user modify permission (i.e., NT AUTHORITY\Authenticated Users:(OI)(CI)(M)) to the contents of the directory and its sub-folders. In addition, the program installs a service called IDriveService that runs as LocalSystem. Thus, any standard user can escalate privileges to NT AUTHORITY\SYSTEM by substituting the service's binary with a malicious one.	7.8	More Details
CVE-2020-9586	Adobe Character Animator versions 3.2 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9589	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-14482	Delta Industrial Automation DOPSoft, Version 4.00.08.15 and prior. Opening a specially crafted project file may overflow the heap, which may allow remote code execution, disclosure/modification of information, or cause the application to crash.	7.8	More Details
CVE-2020-9590	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9621	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-3969	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an off-by-one heap-overflow vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible.	7.8	More Details
CVE-2020-3768	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a dll search-order hijacking vulnerability. Successful exploitation could lead to privilege escalation.	7.8	More Details
CVE-2020-9554	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9555	Adobe Bridge versions 10.0.1 and earlier version have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9556	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9559	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9605	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-8019	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1.	7.7	More Details
CVE-2020-8014	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of kopano-spamd of openSUSE Leap 15.1, openSUSE Tumbleweed allowed local attackers with the privileges of the kopano user to escalate to root. This issue affects: openSUSE Leap 15.1 kopano-spamd versions prior to 10.0.5-lp151.4.1. openSUSE Tumbleweed kopano-spamd versions prior to 10.0.5-1.1.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8022	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.	7.7	More Details
CVE-2020-15084	In express-jwt (NPM package) up and including version 5.3.3, the algorithms entry to be specified in the configuration is not being enforced. When algorithms is not specified in the configuration, with the combination of jwks-rsa, it may lead to authorization bypass. You are affected by this vulnerability if all of the following conditions apply: - You are using express-jwt - You do not have **algorithms** configured in your express-jwt configuration. - You are using libraries such as jwks-rsa as the **secret**. You can fix this by specifying **algorithms** in the express-jwt configuration. See linked GHSA for example. This is also fixed in version 6.0.0.	7.7	More Details
CVE-2020-11961	Xiaomi router R3600 ROM before 1.0.50 is affected by a sensitive information leakage caused by an insecure interface get_config_result without authentication	7.5	More Details
CVE-2020-15336	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has no authentication for /cnr requests.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10624	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes a session token on the network.	7.5	More Details
CVE-2020-10628	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes unencrypted passwords on the network.	7.5	More Details
CVE-2020-11996	A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.	7.5	More Details
CVE-2020-13891	An issue was discovered in Mattermost Mobile Apps before 1.31.2 on iOS. Unintended third-party servers could sometimes obtain authorization tokens, aka MMSA-2020-0022.	7.5	More Details
CVE-2020-4044	The xrdp-sesman service before version 0.9.13.1 can be crashed by connecting over port 3350 and supplying a malicious payload. Once the xrdp-sesman process is dead, an unprivileged attacker on the server could then proceed to start their own imposter sesman service listening on port 3350. This will allow them to capture any user credentials that are submitted to XRDP and approve or reject arbitrary login credentials. For xorgxrdp sessions in particular, this allows an unauthorized user to hijack an existing session. This is a buffer overflow attack, so there may be a risk of arbitrary code execution as well.	7.5	More Details
CVE-2020-11959	An unsafe configuration of nginx lead to information leak in Xiaomi router R3600 ROM before 1.0.50.	7.5	More Details
CVE-2020-9494	Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.10, and 8.0.0 to 8.0.7 is vulnerable to certain types of HTTP/2 HEADERS frames that can cause the server to allocate a large amount of memory and spin the thread.	7.5	More Details
CVE-2020-9623	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-4452	IBM API Connect V2018.4.1.0 through 2018.4.1.11 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 181324.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12048	Phoenix Hemodialysis Delivery System SW 3.36 and 3.40, The Phoenix Hemodialysis device does not support data-in-transit encryption (e.g., TLS/SSL) when transmitting treatment and prescription data on the network between the Phoenix system and the Exalis dialysis data management tool. An attacker with access to the network could observe sensitive treatment and prescription data sent between the Phoenix system and the Exalis tool.	7.5	More Details
CVE-2020-12037	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device.	7.5	More Details
CVE-2020-14017	An issue was discovered in Navigate CMS 2.9 r1433. Sessions, as well as associated information such as CSRF tokens, are stored in cleartext files in the directory /private/sessions. An unauthenticated user could use a brute-force approach to attempt to identify existing sessions, or view the contents of this file to discover details about a session.	7.5	More Details
CVE-2020-12036	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device.	7.5	More Details
CVE-2020-14015	An issue was discovered in Navigate CMS 2.9 r1433. When performing a password reset, a user is emailed an activation code that allows them to reset their password. There is, however, a flaw when no activation code is supplied. The system will allow an unauthorized user to continue setting a password, even though no activation code was supplied, setting the password for the most recently created user in the system (the user with the highest user id).	7.5	More Details
CVE-2020-13700	An issue was discovered in the acf-to-rest-api plugin through 3.1.0 for WordPress. It allows an insecure direct object reference via permalinks manipulation, as demonstrated by a wp-json/acf/v3/options/ request that reads sensitive information in the wp_options table, such as the login and pass values.	7.5	More Details
CVE-2020-14058	An issue was discovered in Squid before 4.12 and 5.x before 5.0.3. Due to use of a potentially dangerous function, Squid and the default certificate validation helper are vulnerable to a Denial of Service when opening a TLS connection to an attacker-controlled server for HTTPS. This occurs because unrecognized error values are mapped to NULL, but later code expects that each error value is mapped to a valid error string.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14474	The Cellebrite UFED physical device 5.0 through 7.5.0.845 relies on key material hardcoded within both the executable code supporting the decryption process, and within the encrypted files themselves by using a key enveloping technique. The recovered key material is the same for every device running the same version of the software, and does not appear to be changed with each new build. It is possible to reconstruct the decryption process using the hardcoded key material and obtain easy access to otherwise protected data.	7.5	More Details
CVE-2020-7667	In package github.com/sassoftware/go-rpmutils/cpio before version 0.1.0, the CPIO extraction functionality doesn't sanitize the paths of the archived files for leading and non-leading ".." which leads in file extraction outside of the current directory. Note: the fixing commit was applied to all affected versions which were re-released.	7.5	More Details
CVE-2020-9587	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an authorization bypass vulnerability. Successful exploitation could lead to potentially unauthorized product discounts.	7.5	More Details
CVE-2020-9591	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to unauthorized access to admin panel.	7.5	More Details
CVE-2020-9625	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-9627	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-9628	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-10280	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard.	7.5	More Details
CVE-2020-12008	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems use cleartext messages to communicate order information with an order entry system. This could allow an attacker with network access to view sensitive data including PHI.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20413	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability on the UserPickerBrowser.jspa page. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	7.5	More Details
CVE-2020-15335	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has no authentication for /registerCpe requests.	7.5	More Details
CVE-2020-10273	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data.	7.5	More Details
CVE-2020-3966	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a heap-overflow due to a race condition issue in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible.	7.5	More Details
CVE-2020-9599	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-5602	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19163	A Vulnerability in the firmware of COMMAX WallPad(CDP-1020MB) allow an unauthenticated adjacent attacker to execute arbitrary code, because of a using the old version of MySQL.	7.5	More Details
CVE-2019-19506	Tenda PA6 Wi-Fi Powerline extender 1.0.1.21 is vulnerable to a denial of service, caused by an error in the "homeplugd" process. By sending a specially crafted UDP packet, an attacker could exploit this vulnerability to cause the device to reboot.	7.5	More Details
CVE-2019-3681	A External Control of File Name or Path vulnerability in osc of SUSE Linux Enterprise Module for Development Tools 15, SUSE Linux Enterprise Software Development Kit 12-SP5, SUSE Linux Enterprise Software Development Kit 12-SP4; openSUSE Leap 15.1, openSUSE Factory allowed remote attackers that can change downloaded packages to overwrite arbitrary files. This issue affects: SUSE Linux Enterprise Module for Development Tools 15 osc versions prior to 0.169.1-3.20.1. SUSE Linux Enterprise Software Development Kit 12-SP5 osc versions prior to 0.162.1-15.9.1. SUSE Linux Enterprise Software Development Kit 12-SP4 osc versions prior to 0.162.1-15.9.1. openSUSE Leap 15.1 osc versions prior to 0.169.1-lp151.2.15.1. openSUSE Factory osc versions prior to 0.169.0 .	7.5	More Details
CVE-2020-5603	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors.	7.5	More Details
CVE-2020-9601	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9600	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-3967	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a heap-overflow vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible.	7.5	More Details
CVE-2020-15302	In Argent RecoveryManager before 0xdc350d09f71c48c5D22fBE2741e4d6A03970E192, the executeRecovery function does not require any signatures in the zero-guardian case, which allows attackers to cause a denial of service (locking) or a takeover.	7.5	More Details
CVE-2020-9483	**Resolved** When use H2/MySQL/TiDB as Apache SkyWalking storage, the metadata query through GraphQL protocol, there is a SQL injection vulnerability, which allows to access unpexcted data. Apache SkyWalking 6.0.0 to 6.6.0, 7.0.0 H2/MySQL/TiDB storage implementations don't use the appropriate way to set SQL parameters.	7.5	More Details
CVE-2020-5584	Cybozu Garoon 4.0.0 to 5.0.1 allow remote attackers to obtain unintended information via unspecified vectors.	7.5	More Details
CVE-2020-15087	In Presto before version 337, authenticated users can bypass authorization checks by directly accessing internal APIs. This impacts Presto server installations with secure internal communication configured. This does not affect installations that have not configured secure internal communication, as these installations are inherently insecure. This only affects Presto server installations. This does NOT affect clients such as the CLI or JDBC driver. This vulnerability has been fixed in version 337. Additionally, this issue can be mitigated by blocking network access to internal APIs on the coordinator and workers.	7.4	More Details
CVE-2020-7049	Nozomi Networks OS before 19.0.4 allows /#/network?tab=network_node_list.html CSV Injection.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13247	BooleBox Secure File Sharing Utility before 4.2.3.0 allows CSV injection via a crafted user name that is mishandled during export from the activity logs in the Audit Area.	7.3	More Details
CVE-2020-9588	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass.	7.2	More Details
CVE-2020-15308	Support Incident Tracker (aka SiT! or SiTracker) 3.67 p2 allows post-authentication SQL injection via the site_edit.php typeid or site parameter, the search_incidents_advanced.php search_title parameter, or the report_qbe.php criteriafield parameter.	7.2	More Details
CVE-2019-19161	CyMiInstaller322 ActiveX which runs MIPLATFORM downloads files required to run applications. A vulnerability in downloading files by CyMiInstaller322 ActiveX caused by an attacker to download randomly generated DLL files and MIPLATFORM to load those DLLs due to insufficient verification.	7.2	More Details
CVE-2020-10274	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database.	7.1	More Details
CVE-2020-5970	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which an input data size is not validated, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	7.1	More Details
CVE-2020-5972	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which local pointer variables are not initialized and may be freed later, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	7.1	More Details
CVE-2020-7816	A vulnerability in the JPEG image parsing module in DaView Indy, DaVa+, DaOffice softwares could allow an unauthenticated, remote attacker to cause an arbitrary code execution on an affected device.nThe vulnerability is due to a stack overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9615	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a race condition vulnerability. Successful exploitation could lead to security feature bypass.	7.0	More Details
CVE-2020-4067	In coturn before version 4.5.1.3, there is an issue whereby STUN/TURN response buffer is not initialized properly. There is a leak of information between different client connections. One client (an attacker) could use their connection to intelligently query coturn to get interesting bytes in the padding bytes from the connection of another client. This has been fixed in 4.5.1.3.	7.0	More Details
CVE-2020-15085	In Saleor Storefront before version 2.10.3, request data used to authenticate customers was inadvertently cached in the browser's local storage mechanism, including credentials. A malicious user with direct access to the browser could extract the email and password. In versions prior to 2.10.0 persisted the cache even after the user logged out. This is fixed in version 2.10.3. A workaround is to manually clear application data (browser's local storage) after logging into Saleor Storefront.	6.9	More Details
CVE-2020-9047	A vulnerability exists that could allow the execution of unauthorized code or operating system commands on systems running exacqVision Web Service versions 20.06.3.0 and prior and exacqVision Enterprise Manager versions 20.06.4.0 and prior. An attacker with administrative privileges could potentially download and run a malicious executable that could allow OS command injection on the system.	6.8	More Details
CVE-2013-7489	The Beaker library through 1.11.0 for Python is affected by deserialization of untrusted data, which could lead to arbitrary code execution.	6.8	More Details
CVE-2020-14069	An issue was discovered in MK-AUTH 19.01. There are SQL injection issues in mkt/ PHP scripts, as demonstrated by arp.php, dhcp.php, hotspot.php, ip.php, pgaviso.php, pgcorte.php, pppoe.php, queues.php, and wifi.php.	6.8	More Details
CVE-2020-3767	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an insufficient input validation vulnerability. Successful exploitation could lead to application-level denial-of-service (dos).	6.5	More Details
CVE-2020-15018	playSMS through 1.4.3 is vulnerable to session fixation.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5583	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to obtain unauthorized Multi-Report's data via unspecified vectors.	6.5	More Details
CVE-2020-5581	Path traversal vulnerability in Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to obtain unintended information via unspecified vectors.	6.5	More Details
CVE-2020-5587	Cybozu Garoon 4.0.0 to 5.0.1 allow remote authenticated attackers to obtain unintended information via unspecified vectors.	6.5	More Details
CVE-2020-3798	Adobe Digital Editions versions 4.5.11.187212 and below have a file enumeration (host or local network) vulnerability. Successful exploitation could lead to information disclosure.	6.5	More Details
CVE-2020-3796	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an improper access control vulnerability. Successful exploitation could lead to system file structure disclosure.	6.5	More Details
CVE-2020-15389	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and invalid files in a directory operated on by the decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice.	6.5	More Details
CVE-2020-14059	An issue was discovered in Squid 5.x before 5.0.3. Due to an Incorrect Synchronization, a Denial of Service can occur when processing objects in an SMP cache because of an Ipc::Mem::PageStack::pop ABA problem during access to the memory page/slot management list.	6.5	More Details
CVE-2019-20892	net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.	6.5	More Details
CVE-2019-20410	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view sensitive information via an Information Disclosure vulnerability in the comment restriction feature. The affected versions are before version 7.6.17, from version 7.7.0 before 7.13.9, and from version 8.0.0 before 8.4.2.	6.5	More Details
CVE-2020-15043	iBall WRB303N devices allow CSRF attacks, as demonstrated by enabling remote management, enabling DHCP, or modifying the subnet range for IP addresses.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4089	HCL Notes is vulnerable to an information leakage vulnerability through its support for the 'mailto' protocol. This vulnerability could result in files from the user's filesystem or connected network filesystems being leaked to a third party. All versions of HCL Notes 9, 10 and 11 are affected.	6.5	More Details
CVE-2020-8573	The NetApp HCI H610C, H615C and H610S Baseboard Management Controllers (BMC) are shipped with a documented default account and password that should be changed during the initial node setup. During upgrades to Element 11.8 and 12.0 or the Compute Firmware Bundle 12.2.92 the BMC account password on the H610C, H615C and H610S platforms is reset to the default documented value which could allow remote attackers to cause a Denial of Service (DoS).	6.5	More Details
CVE-2020-15365	LibRaw before 0.20-Beta3 has an out-of-bounds write in parse_exif() in metadata\exif_gps.cpp via an unrecognized AtomName and a zero value of tiff_nifds.	6.5	More Details
CVE-2020-10277	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine.	6.4	More Details
CVE-2019-4650	IBM Maximo Asset Management 7.6.1.1 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 170961.	6.3	More Details
CVE-2020-9413	The MFT Browser file transfer client and MFT Browser admin client components of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contain a vulnerability that theoretically allows an attacker to craft an URL that will execute arbitrary commands on the affected system. If the attacker convinces an authenticated user with a currently active session to enter or click on the URL the commands will be executed on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below.	6.3	More Details
CVE-2020-5969	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which it validates a shared resource before using it, creating a race condition which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15364	The Nexos theme through 1.7 for WordPress allows top-map/?search_location= reflected XSS.	6.1	More Details
CVE-2020-4323	IBM Security Secret Server 10.7 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: 177514.	6.1	More Details
CVE-2020-12020	Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13 and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 does not restrict non administrative users from gaining access to the operating system and editing the application startup script. Successful exploitation of this vulnerability may allow an attacker to alter the startup script as the limited-access user.	6.1	More Details
CVE-2020-9581	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	6.1	More Details
CVE-2020-9577	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure .	6.1	More Details
CVE-2020-12012	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13, and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 have hard-coded administrative account credentials for the ExactaMix application. Successful exploitation of this vulnerability may allow an attacker with physical access to gain unauthorized access to view/update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.	6.1	More Details
CVE-2020-14413	NeDi 1.9C is vulnerable to XSS because of an incorrect implementation of sanitize() in inc/libmisc.php. This function attempts to escape the SCRIPT tag from user-controllable values, but can be easily bypassed, as demonstrated by an onerror attribute of an IMG element as a Devices-Config.php?sta= value.	6.1	More Details
CVE-2020-15307	Nozomi Guardian before 19.0.4 allows attackers to achieve stored XSS (in the web front end) by leveraging the ability to create a custom field with a crafted field name.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12635	XSS exists in the WebForms Pro M2 extension before 2.9.17 for Magento 2 via the textarea field.	6.1	More Details
CVE-2020-14071	An issue was discovered in MK-AUTH 19.01. XSS vulnerabilities in admin and client scripts allow an attacker to execute arbitrary JavaScript code.	6.1	More Details
CVE-2020-15016	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Other-Converter.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the txt GET parameter.	6.1	More Details
CVE-2020-15017	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Devices-Config.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the sta GET parameter.	6.1	More Details
CVE-2020-7354	Cross-site Scripting (XSS) vulnerability in the 'host' field of a discovered scan asset in Rapid7 Metasploit Pro allows an attacker with a specially-crafted network service of a scan target to store an XSS sequence in the Metasploit Pro console, which will trigger when the operator views the record of that scanned host in the Metasploit Pro interface. This issue affects Rapid7 Metasploit Pro version 4.17.1-20200427 and prior versions, and is fixed in Metasploit Pro version 4.17.1-20200514. See also CVE-2020-7355, which describes a similar issue, but involving the generated 'notes' field of a discovered scan asset.	6.1	More Details
CVE-2020-7355	Cross-site Scripting (XSS) vulnerability in the 'notes' field of a discovered scan asset in Rapid7 Metasploit Pro allows an attacker with a specially-crafted network service of a scan target store an XSS sequence in the Metasploit Pro console, which will trigger when the operator views the record of that scanned host in the Metasploit Pro interface. This issue affects Rapid7 Metasploit Pro version 4.17.1-20200427 and prior versions, and is fixed in Metasploit Pro version 4.17.1-20200514. See also CVE-2020-7354, which describes a similar issue, but involving the generated 'host' field of a discovered scan asset.	6.1	More Details
CVE-2020-14018	An issue was discovered in Navigate CMS 2.9 r1433. There is a stored XSS vulnerability that is executed on the page to view users, and on the page to edit users. This is present in both the User field and the E-Mail field. On the Edit user page, the XSS is only triggered via the E-Mail field; however, on the View user page the XSS is triggered via either the User field or the E-Mail field.	6.1	More Details
CVE-2020-15015	The FileExplorer component in GleamTech FileUltimate 6.1.5.0 allows XSS via an SVG document.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-13483	The Web Application Firewall in Bitrix24 through 20.0.0 allows XSS via the items[ITEMS][ID] parameter to the components/bitrix/mobileapp.list/ajax.php/ URI.	6.1	More Details
CVE-2020-12024	Baxter ExactaMix EM 2400 versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 does not restrict access to the USB interface from an unauthorized user with physical access. Successful exploitation of this vulnerability may allow an attacker with physical access to the system the ability to load an unauthorized payload or unauthorized access to the hard drive by booting a live USB OS. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.	6.1	More Details
CVE-2020-15316	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account within the /opt/axess chroot directory tree.	5.9	More Details
CVE-2020-15312	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account.	5.9	More Details
CVE-2020-15319	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/mysql chroot directory tree.	5.9	More Details
CVE-2020-4565	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow an attacker to obtain sensitive information due to insecure communications being used between the application and server. IBM X-Force ID: 183935.	5.9	More Details
CVE-2020-15318	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account within the /opt/mysql chroot directory tree.	5.9	More Details
CVE-2020-15047	MSA/SMTP.cpp in Trojita before 0.8 ignores certificate-verification errors, which allows man-in-the-middle attackers to spoof SMTP servers.	5.9	More Details
CVE-2020-15317	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/axess chroot directory tree.	5.9	More Details
CVE-2020-14002	PuTTY 0.68 through 0.73 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15315	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account within the /opt/axess chroot directory tree.	5.9	More Details
CVE-2020-15314	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account.	5.9	More Details
CVE-2020-14145	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.	5.9	More Details
CVE-2020-4413	IBM Security Secret Server 10.7 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 179988.	5.9	More Details
CVE-2020-15313	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account.	5.9	More Details
CVE-2019-19160	Reportexpress ProPlus contains a vulnerability that could allow an arbitrary code execution by inserted VBscript into the configure file(rxp).	5.7	More Details
CVE-2020-12866	A NULL pointer dereference in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to cause a denial of service, GHSL-2020-079.	5.7	More Details
CVE-2020-13657	An elevation of privilege vulnerability exists in Avast Free Antivirus and AVG AntiVirus Free before 20.4 due to improperly handling hard links. The vulnerability allows local users to take control of arbitrary files.	5.5	More Details
CVE-2020-15368	AsrDrv103.sys in the ASRock RGB Driver does not properly restrict access from user space, as demonstrated by triggering a triple fault via a request to zero CR3.	5.5	More Details
CVE-2020-15393	In the Linux kernel 4.4 through 5.7.6, usbtest_disconnect in drivers/usb/misc/usbtest.c has a memory leak, aka CID-28ebeb8db770.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9617	Adobe Premiere Rush versions 1.5.8 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9595	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9616	Adobe Premiere Pro versions 14.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-3965	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the XHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine.	5.5	More Details
CVE-2020-10769	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service.	5.5	More Details
CVE-2020-10727	A flaw was found in ActiveMQ Artemis management API from version 2.7.0 up until 2.12.0, where a user inadvertently stores passwords in plaintext in the Artemis shadow file (etc/artemis-users.properties file) when executing the `resetUsers` operation. A local attacker can use this flaw to read the contents of the Artemis shadow file.	5.5	More Details
CVE-2020-3971	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201907101-SG), Workstation (15.x before 15.0.2), and Fusion (11.x before 11.0.2) contain a heap overflow vulnerability in the vmxnet3 virtual network adapter. A malicious actor with local access to a virtual machine with a vmxnet3 network adapter present may be able to read privileged information contained in physical memory.	5.5	More Details
CVE-2020-15306	An issue was discovered in OpenEXR before v2.5.2. Invalid chunkCount attributes could cause a heap buffer overflow in getChunkOffsetTableSize() in IlmImf/ImfMisc.cpp.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15305	An issue was discovered in OpenEXR before 2.5.2. Invalid input could cause a use-after-free in DeepScanLineInputFile::DeepScanLineInputFile() in IlmImf/ImfDeepScanLineInputFile.cpp.	5.5	More Details
CVE-2020-15304	An issue was discovered in OpenEXR before 2.5.2. An invalid tiled input file could cause invalid memory access in TiledInputFile::TiledInputFile() in IlmImf/ImfTiledInputFile.cpp, as demonstrated by a NULL pointer dereference.	5.5	More Details
CVE-2020-9618	Adobe Audition versions 13.0.5 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-10177	Pillow before 7.1.0 has multiple out-of-bounds reads in libImaging/FliDecode.c.	5.5	More Details
CVE-2020-10378	In libImaging/PcxDecode.c in Pillow before 7.1.0, an out-of-bounds read can occur when reading PCX files where state->shuffle is instructed to read beyond state->buffer.	5.5	More Details
CVE-2020-10994	In libImaging/Jpeg2KDecode.c in Pillow before 7.1.0, there are multiple out-of-bounds reads via a crafted JP2 file.	5.5	More Details
CVE-2020-9611	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service.	5.5	More Details
CVE-2020-9610	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a null pointer vulnerability. Successful exploitation could lead to application denial-of-service.	5.5	More Details
CVE-2020-9609	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9608	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9666	Adobe Campaign Classic before 20.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9603	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9602	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9598	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9593	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-14955	In Jiangmin Antivirus 16.0.13.129, the driver file (KVFG.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220440.	5.5	More Details
CVE-2020-9622	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-3963	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a use-after-free vulnerability in PVNVRAM. A malicious actor with local access to a virtual machine may be able to read privileged information contained in physical memory.	5.5	More Details
CVE-2020-9629	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-3809	Adobe After Effects versions 17.0.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5965	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service.	5.5	More Details
CVE-2020-15358	In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.	5.5	More Details
CVE-2020-9557	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9624	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	5.5	More Details
CVE-2020-9584	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	5.4	More Details
CVE-2020-15006	Bludit 3.12.0 allows stored XSS via JavaScript code in an SVG document to bl-kernel/ajax/logo-upload.php.	5.4	More Details
CVE-2020-14006	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows XSS via a Responsible Team.	5.4	More Details
CVE-2020-14007	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows XSS via a name of an alert definition.	5.4	More Details
CVE-2020-14014	An issue was discovered in Navigate CMS 2.8 and 2.9 r1433. The query parameter fid on the resource navigate.php does not perform sufficient data validation and/or encoding, making it vulnerable to reflected XSS.	5.4	More Details
CVE-2020-13248	BooleBox Secure File Sharing Utility before 4.2.3.0 allows stored XSS via a crafted avatar field within My Account JSON data to Account.aspx.	5.4	More Details
CVE-2020-15038	The SeedProd coming-soon plugin before 5.1.1 for WordPress allows XSS.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4223	IBM Maximo Asset Management 7.6.0.10 and 7.6.1.1 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: 175121.	5.4	More Details
CVE-2020-10753	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue.	5.4	More Details
CVE-2020-4557	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 are 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: 183611.	5.4	More Details
CVE-2019-20414	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in Issue Navigator Basic Search. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	5.4	More Details
CVE-2020-14016	An issue was discovered in Navigate CMS 2.9 r1433. The forgot-password feature allows users to reset their passwords by using either their username or the email address associated with their account. However, the feature returns a not_found message when the provided username or email address does not match a user in the system. This can be used to enumerate users.	5.3	More Details
CVE-2020-4072	In generator-jhipster-kotlin version 1.6.0 log entries are created for invalid password reset attempts. As the email is provided by a user and the api is public this can be used by an attacker to forge log entries. This is vulnerable to https://cwe.mitre.org/data/definitions/117.html This problem affects only application generated with jwt or session authentication. Applications using oauth are not vulnerable. This issue has been fixed in version 1.7.0.	5.3	More Details
CVE-2020-4342	IBM Security Secret Server 10.7 could disclose sensitive information included in installation files to an unauthorized user. IBM X-Force ID: 178182.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4341	IBM Security Secret Server 10.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 178181.	5.3	More Details
CVE-2020-4327	IBM Security Secret Server 10.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 177599.	5.3	More Details
CVE-2020-11735	The private-key operations in ecc.c in wolfSSL before 4.4.0 do not use a constant-time modular inverse when mapping to affine coordinates, aka a "projective coordinates leak."	5.3	More Details
CVE-2020-8024	A Incorrect Default Permissions vulnerability in the packaging of hylafax+ of openSUSE Leap 15.2, openSUSE Leap 15.1, openSUSE Factory allows local attackers to escalate from user uucp to users calling hylafax binaries. This issue affects: openSUSE Leap 15.2 hylafax+ versions prior to 7.0.2-lp152.2.1. openSUSE Leap 15.1 hylafax+ version 5.6.1-lp151.3.7 and prior versions. openSUSE Factory hylafax+ versions prior to 7.0.2-2.1.	5.3	More Details
CVE-2019-20412	The Convert Sub-Task to Issue page in affected versions of Atlassian Jira Server and Data Center allow remote attackers to enumerate the following information via an Improper Authentication vulnerability: Workflow names; Project Key, if it is part of the workflow name; Issue Keys; Issue Types; Status Types. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	5.3	More Details
CVE-2020-13896	The web interface of Maipu MP1800X-50 7.5.3.14(R) devices allows remote attackers to obtain sensitive information via the form/formDeviceVerGet URI, such as system id, hardware model, hardware version, bootloader version, software version, software image file, compilation time, and system uptime. This is similar to CVE-2019-1653.	5.3	More Details
CVE-2020-5588	Path traversal vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to obtain unintended information via unspecified vectors.	4.9	More Details
CVE-2020-15026	Bludit 3.12.0 allows admins to use a /plugin-backup-download?file=../ directory traversal approach for arbitrary file download via backup/plugin.php.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12035	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The PrismaFlex device contains a hard-coded service password that provides access to biomedical information, device settings, calibration settings, and network configuration. This could allow an attacker to modify device settings and calibration.	4.9	More Details
CVE-2019-20416	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the project configuration feature. The affected versions are before version 8.3.0.	4.8	More Details
CVE-2020-15041	PHP-Fusion 9.03.60 allows XSS via the administration/site_links.php Add Site Link field.	4.8	More Details
CVE-2020-5586	Cross-site scripting vulnerability in Cybozu Garoon 4.10.3 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.	4.8	More Details
CVE-2020-5585	Cross-site scripting vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors.	4.8	More Details
CVE-2020-9437	SecureAuth.aspx in SecureAuth IdP 9.3.0 suffers from a client-side template injection that allows for script execution, in the same manner as XSS.	4.8	More Details
CVE-2020-13423	Form Builder 2.1.0 for Magento has multiple XSS issues that can be exploited against Magento 2 admin accounts via the Current_url or email field, or the User-Agent HTTP header.	4.8	More Details
CVE-2020-3964	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the EHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in the hypervisor's memory. Additional conditions beyond the attacker's control need to be present for exploitation to be possible.	4.7	More Details
CVE-2020-5967	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18256	BIOTRONIK CardioMessenger II, The affected products use individual per-device credentials that are stored in a recoverable format. An attacker with physical access to the CardioMessenger can use these credentials for network authentication and decryption of local data in transit.	4.6	More Details
CVE-2019-18254	BIOTRONIK CardioMessenger II, The affected products do not encrypt sensitive information while at rest. An attacker with physical access to the CardioMessenger can disclose medical measurement data and the serial number from the implanted cardiac device the CardioMessenger is paired with.	4.6	More Details
CVE-2020-10278	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image.	4.6	More Details
CVE-2020-15025	ntpd in ntp 4.2.8 before 4.2.8p15 and 4.3.x before 4.3.101 allows remote attackers to cause a denial of service (memory consumption) by sending packets, because memory is not freed in situations where a CMAC key is used and associated with a CMAC algorithm in the ntp.keys file.	4.4	More Details
CVE-2020-5973	NVIDIA Virtual GPU Manager and the guest drivers contain a vulnerability in vGPU plugin, in which there is the potential to execute privileged operations, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).	4.4	More Details
CVE-2020-15401	IOBit Malware Fighter Pro 8.0.2.547 allows local users to gain privileges for file deletion by manipulating malicious flagged file locations with an NTFS junction and an Object Manager symbolic link.	4.4	More Details
CVE-2020-14477	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information.	4.4	More Details
CVE-2020-12863	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-083.	4.3	More Details
CVE-2020-12862	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-082.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-18248	BIOTRONIK CardioMessenger II, The affected products transmit credentials in clear-text prior to switching to an encrypted communication channel. An attacker can disclose the product’s client credentials for connecting to the BIOTRONIK Remote Communication infrastructure.	4.3	More Details
CVE-2019-18252	BIOTRONIK CardioMessenger II, The affected products allow credential reuse for multiple authentication purposes. An attacker with adjacent access to the CardioMessenger can disclose its credentials used for connecting to the BIOTRONIK Remote Communication infrastructure.	4.3	More Details
CVE-2020-4322	IBM Security Secret Server 10.7 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 177511.	4.3	More Details
CVE-2020-5582	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to alter the data for the file attached to Report via unspecified vectors.	4.3	More Details
CVE-2020-15011	GNU Mailman before 2.1.33 allows arbitrary content injection via the Cgi/private.py private archive login page.	4.3	More Details
CVE-2019-20411	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify Wallboard settings via a Cross-site request forgery (CSRF) vulnerability. The affected versions are before version 7.13.9, and from version 8.0.0 before 8.4.2.	4.3	More Details
CVE-2019-18246	BIOTRONIK CardioMessenger II, The affected products do not properly enforce mutual authentication with the BIOTRONIK Remote Communication infrastructure.	4.3	More Details
CVE-2020-4037	In OAuth2 Proxy from version 5.1.1 and less than version 6.0.0, users can provide a redirect address for the proxy to send the authenticated user to at the end of the authentication flow. This is expected to be the original URL that the user was trying to access. This redirect URL is checked within the proxy and validated before redirecting the user to prevent malicious actors providing redirects to potentially harmful sites. This has been fixed in version 6.0.0.	4.3	More Details
CVE-2019-20415	Atlassian Jira Server and Data Center in affected versions allows remote attackers to modify logging and profiling settings via a cross-site request forgery (CSRF) vulnerability. The affected versions are before version 7.13.3, and from version 8.0.0 before 8.1.0.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15400	CakePHP before 4.0.6 mishandles CSRF token generation. This might be remotely exploitable in conjunction with XSS.	4.3	More Details
CVE-2020-15412	An issue was discovered in MISP 2.4.128. app/Controller/EventsController.php lacks an event ACL check before proceeding to allow a user to send an event contact form.	4.3	More Details
CVE-2020-12864	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-081.	4.3	More Details
CVE-2020-3970	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds read vulnerability in the Shader functionality. A malicious actor with non-administrative local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to crash the virtual machine's vmx process leading to a partial denial of service condition.	3.8	More Details
CVE-2020-9558	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	3.3	More Details
CVE-2020-9626	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	3.3	More Details
CVE-2020-9553	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	3.3	More Details
CVE-2020-15005	In MediaWiki before 1.31.8, 1.32.x and 1.33.x before 1.33.4, and 1.34.x before 1.34.2, private wikis behind a caching server using the img_auth.php image authorization security feature may have had their files cached publicly, so any unauthorized user could view them. This occurs because Cache-Control and Vary headers were mishandled.	3.1	More Details
CVE-2020-12039	Baxter Sigma Spectrum Infusion Pumps Sigma Spectrum Infusion System v's6.x model 35700BAX & Baxter Spectrum Infusion System v's8.x model 35700BAX2 contain hardcoded passwords when physically entered on the keypad provide access to biomedical menus including device settings, view calibration values, network configuration of Sigma Spectrum WBM if installed.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4071	In django-basic-auth-ip-whitelist before 0.3.4, a potential timing attack exists on websites where the basic authentication is used or configured, i.e. BASIC_AUTH_LOGIN and BASIC_AUTH_PASSWORD is set. Currently the string comparison between configured credentials and the ones provided by users is performed through a character-by-character string comparison. This enables a possibility that attacker may time the time it takes the server to validate different usernames and password, and use this knowledge to work out the valid credentials. This attack is understood not to be realistic over the Internet. However, it may be achieved from within local networks where the website is hosted, e.g. from inside a data centre where a website's server is located. Sites protected by IP address whitelisting only are unaffected by this vulnerability. This vulnerability has been fixed on version 0.3.4 of django-basic-auth-ip-whitelist. Update to version 0.3.4 as soon as possible and change basic authentication username and password configured on a Django project using this package. A workaround without upgrading to version 0.3.4 is to stop using basic authentication and use the IP whitelisting component only. It can be achieved by not setting BASIC_AUTH_LOGIN and BASIC_AUTH_PASSWORD in Django project settings.	2.2	More Details
CVE-2020-15356	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-15354	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2020-15311	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2008-4080. Reason: This candidate is a duplicate of CVE-2008-4080.2. Notes: All CVE users should reference CVE-2008-4080.2 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2020-15355	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