SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 26 August 2020

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-14500	Secomea GateManager all versions prior to 9.2c, An attacker can send a negative value and overwrite arbitrary data.	10.0	More Details
CVE-2020-24186	A Remote Code Execution vulnerability exists in the gVectors wpDiscuz plugin 7.0 through 7.0.4 for WordPress, which allows unauthenticated users to upload any type of file, including PHP files via the wmuUploadFiles AJAX action.	10.0	More Details
CVE-2020-15149	NodeBB before version 1.14.3 has a bug introduced in version 1.12.2 in the validation logic that makes it possible to change the password of any user on a running NodeBB forum by sending a specially crafted socket.io call to the server. This could lead to a privilege escalation event due via an account takeover. As a workaround you may cherry-pick the following commit from the project's repository to your running instance of NodeBB: 16cee1b03ba3eee177834a1fdac4aa8a12b39d2a. This is fixed in version 1.14.3.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24055	Verint 5620PTZ Verint_FW_0_42 and Verint 4320 V4320_FW_0_23, and V4320_FW_0_31 units feature an autodiscovery service implemented in the binary executable '/usr/sbin/DM' that listens on port TCP 6666. The service is vulnerable to a stack buffer overflow. It is worth noting that this service does not require any authentication.	9.8	More Details
CVE-2020-24054	The administration console of the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units features a 'statusbroadcast' command that can spawn a given process repeatedly at a certain time interval as 'root'. One of the limitations of this feature is that it only takes a path to a binary without arguments; however, this can be circumvented using special shell variables, such as '${IFS}'. As a result, an attacker can execute arbitrary commands as 'root' on the units.	9.8	More Details
CVE-2020-16245	Advantech iView, Versions 5.7 and prior. The affected product is vulnerable to path traversal vulnerabilities that could allow an attacker to create/download arbitrary files, limit system availability, and remotely execute code.	9.8	More Details
CVE-2020-14524	Softing Industrial Automation all versions prior to the latest build of version 4.47.0, The affected product is vulnerable to a heap-based buffer overflow, which may allow an attacker to remotely execute arbitrary code.	9.8	More Details
CVE-2020-14510	GateManager versions prior to 9.2c, The affected product contains a hard-coded credential for telnet, allowing an unprivileged attacker to execute commands as root.	9.8	More Details
CVE-2020-6637	openSIS Community Edition version 7.3 is vulnerable to SQL injection via the USERNAME parameter of index.php.	9.8	More Details
CVE-2020-8234	A vulnerability exists in The EdgeMax EdgeSwitch firmware <v1.9.1 where the EdgeSwitch legacy web interface SIDSSL cookie for admin can be guessed, enabling the attacker to obtain high privileges and get a root shell by a Command injection.	9.8	More Details
CVE-2020-15639	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the decryptFile method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10496.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24051	The Moog EXO Series EXVF5C-2 and EXVP7C2-3 units support the ONVIF interoperability IP-based physical security protocol, which requires authentication for some of its operations. It was found that the authentication check for those ONVIF operations can be bypassed. An attacker can abuse this issue to execute privileged operations without authentication, for instance, to create a new Administrator user.	9.8	More Details
CVE-2020-16279	The Kommbox component in Rangee GmbH RangeeOS 8.0.4 is vulnerable to Remote Code Execution due to untrusted user supplied input being passed to the command line without sanitization.	9.8	More Details
CVE-2020-23935	Kabir Alhasan Student Management System 1.0 is vulnerable to Authentication Bypass via "Username: admin'# && Password: (Write Something)".	9.8	More Details
CVE-2020-23936	PHPGurukul Vehicle Parking Management System 1.0 is vulnerable to Authentication Bypass via "Username: admin'# && Password: (Write Something)".	9.8	More Details
CVE-2020-10283	The Micro Air Vehicle Link (MAVLink) protocol presents authentication mechanisms on its version 2.0 however according to its documentation, in order to maintain backwards compatibility, GCS and autopilot negotiate the version via the AUTOPILOT_VERSION message. Since this negotiation depends on the answer, an attacker may craft packages in a way that hints the autopilot to adopt version 1.0 of MAVLink for the communication. Given the lack of authentication capabilities in such version of MAVLink (refer to CVE-2020-10282), attackers may use this method to bypass authentication capabilities and interact with the autopilot directly.	9.8	More Details
CVE-2020-17456	SEOWON INTECH SLC-130 And SLR-120S devices allow Remote Code Execution via the ipAddr parameter to the system_log.cgi page.	9.8	More Details
CVE-2020-15636	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR R6400, R6700, R7000, R7850, R7900, R8000, RS400, and XR300 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the check_ra service. A crafted raePolicyVersion in a RAE_Policy.json file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9852.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15146	In SyliusResourceBundle before versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4, request parameters injected inside an expression evaluated by `symfony/expression-language` package haven't been sanitized properly. This allows the attacker to access any public service by manipulating that request parameter, allowing for Remote Code Execution. This issue has been patched for versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4. Versions prior to 1.3 were not patched.	9.6	More Details
CVE-2020-24052	Several XML External Entity (XXE) vulnerabilities in the Moog EXO Series EXVF5C-2 and EXVP7C2-3 units allow remote unauthenticated users to read arbitrary files via a crafted Document Type Definition (DTD) in an XML request.	9.1	More Details
CVE-2019-11857	Lack of input sanitization in AceManager of ALEOS before 4.12.0, 4.9.5 and 4.4.9 allows disclosure of sensitive system information.	9.1	More Details
CVE-2020-24589	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML External Entity injection (XXE) attacks.	9.1	More Details
CVE-2020-24590	The Management Console in WSO2 API Manager through 3.1.0 and API Microgateway 2.2.0 allows XML Entity Expansion attacks.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-15645	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the getFileFromURL method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10553.	8.8	More Details
CVE-2020-19889	DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for index.php?dbhcms_pid=-70 can add a user.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17392	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.3-47255. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handler for HOST_IOCTL_SET_KERNEL_SYMBOLS in the prl_hypervisor kext. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-10519.	8.8	More Details
CVE-2020-7831	A vulnerability in the web-based contract management service interface Ebiz4u of INOGARD could allow an victim user to download any file. The attacker is able to use startup menu directory via directory traversal for automatic execution. The victim user need to reboot, however.	8.8	More Details
CVE-2020-10289	Use of unsafe yaml load. Allows instantiation of arbitrary objects. The flaw itself is caused by an unsafe parsing of YAML values which happens whenever an action message is processed to be sent, and allows for the creation of Python objects. Through this flaw in the ROS core package of actionlib, an attacker with local or remote access can make the ROS Master, execute arbitrary code in Python form. Consider yaml.safe_load() instead. Located first in actionlib/tools/library.py:132. See links for more info on the bug.	8.8	More Details
CVE-2020-24364	MineTime through 1.8.5 allows arbitrary command execution via the notes field in a meeting. Could lead to RCE via meeting invite.	8.8	More Details
CVE-2020-17390	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.2-47123. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the hypervisor kernel extension. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-10030.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17389	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the decryptFile method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10502.	8.8	More Details
CVE-2020-17388	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the Tomcat configuration file. The issue results from the lack of proper restriction to the Tomcat admin console. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10799.	8.8	More Details
CVE-2020-17396	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor module. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-11217.	8.8	More Details
CVE-2020-15531	Silicon Labs Bluetooth Low Energy SDK before 2.13.3 has a buffer overflow via packet data. This is an over-the-air remote code execution vulnerability in Bluetooth LE in EFR32 SoCs and associated modules running Bluetooth SDK, supporting Central or Observer roles.	8.8	More Details
CVE-2020-16282	In the default configuration of Rangee GmbH RangeeOS 8.0.4, all components are executed in the context of the privileged root user. This may allow a local attacker to break out of the restricted environment or inject malicious code into the application and fully compromise the operating system.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17399	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-11303.	8.8	More Details
CVE-2020-17387	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the writeObjectToConfigFile method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10565.	8.8	More Details
CVE-2020-15635	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the acsd service, which listens on TCP port 5916 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-9853.	8.8	More Details
CVE-2020-17400	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11304.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15644	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the setAppFileBytes method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10550.	8.8	More Details
CVE-2020-15643	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the saveAsText method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10549.	8.8	More Details
CVE-2020-15642	This vulnerability allows remote attackers to execute arbitrary code on affected installations of installations of Marvell QConvergeConsole 5.5.0.64. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the isHPSmartComponent method of the GWTTestServiceImpl class. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10501.	8.8	More Details
CVE-2020-24572	An issue was discovered in includes/webconsole.php in RaspAP 2.5. With authenticated access, an attacker can use a misconfigured (and virtually unrestricted) web console to attack the underlying OS (Raspberry Pi) running this software, and execute commands on the system (including ones for uploading of files and execution of code).	8.8	More Details
CVE-2020-24057	The management website of the Verint S5120FD Verint_FW_0_42 unit features a CGI endpoint ('ipfilter.cgi') that allows the user to manage network filtering on the unit. This endpoint is vulnerable to a command injection. An authenticated attacker can leverage this issue to execute arbitrary commands as 'root'.	8.8	More Details
CVE-2020-15070	Zulip Server 2.x before 2.1.7 allows eval injection if a privileged attacker were able to write directly to the postgres database, and chose to write a crafted custom profile field value.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14043	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** A Cross Side Request Forgery (CSRF) vulnerability was found in Codiad v1.7.8 and later. The request to download a plugin from the marketplace is only available to admin users and it isn't CSRF protected in components/market/controller.php. This might cause admins to make a vulnerable request without them knowing and result in remote code execution. NOTE: the vendor states "Codiad is no longer under active maintenance by core contributors."	8.8	More Details
CVE-2020-24614	Fossil before 2.10.2, 2.11.x before 2.11.2, and 2.12.x before 2.12.1 allows remote authenticated users to execute arbitrary code. An attacker must have check-in privileges on the repository.	8.8	More Details
CVE-2020-13826	A CSV injection (aka Excel Macro Injection or Formula Injection) issue in i-doit 1.14.2 allows an attacker to execute arbitrary commands via a Title parameter that is mishandled in a CSV export.	8.8	More Details
CVE-2020-5417	Cloud Foundry CAPI (Cloud Controller), versions prior to 1.97.0, when used in a deployment where an app domain is also the system domain (which is true in the default CF Deployment manifest), were vulnerable to developers maliciously or accidentally claiming certain sensitive routes, potentially resulting in the developer's app handling some requests that were expected to go to certain system components.	8.8	More Details
CVE-2020-24606	Squid before 4.13 and 5.x before 5.0.4 allows a trusted peer to perform Denial of Service by consuming all available CPU cycles during handling of a crafted Cache Digest response message. This only occurs when cache_peer is used with the cache digests feature. The problem exists because peerDigestHandleReply() livelocking in peer_digest.cc mishandles EOF.	8.6	More Details
CVE-2020-15147	Red Discord Bot before versions 3.3.12 and 3.4 has a Remote Code Execution vulnerability in the Streams module. This exploit allows Discord users with specifically crafted "going live" messages to inject code into the Streams module's going live message. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. As a workaround, unloading the Trivia module with `unload streams` can render this exploit not accessible. It is highly recommended updating to 3.3.12 or 3.4 to completely patch this issue.	8.5	More Details
CVE-2020-15140	In Red Discord Bot before version 3.3.11, a RCE exploit has been discovered in the Trivia module: this exploit allows Discord users with specifically crafted usernames to inject code into the Trivia module's leaderboard command. By abusing this exploit, it's possible to perform destructive actions and/or access sensitive information. This critical exploit has been fixed on version 3.3.11.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17395	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the prl_naptd process. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11134.	8.2	More Details
CVE-2020-17397	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the handling of network packets. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11253.	8.2	More Details
CVE-2019-11855	An RPC server is enabled by default on the gateway's LAN of ALEOS before 4.12.0, 4.9.5, and 4.4.9.	8.1	More Details
CVE-2020-19886	DBHcms v1.2.0 has no CSRF protection mechanism,as demonstrated by CSRF for an /index.php?dbhcms_pid=-80&deletemenu=9 can delete any menu.	8.1	More Details
CVE-2019-11862	The SSH service on ALEOS before 4.12.0, 4.9.5, 4.4.9 allows traffic proxying.	8.1	More Details
CVE-2020-7377	The Metasploit Framework module "auxiliary/admin/http/telpho10_credential_dump" module is affected by a relative path traversal vulnerability in the untar method which can be exploited to write arbitrary files to arbitrary locations on the host file system when the module is run on a malicious HTTP server.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7710	This affects all versions of package safe-eval. It is possible for an attacker to run an arbitrary command on the host machine.	8.1	More Details
CVE-2020-24616	FasterXML jackson-databind 2.x before 2.9.10.6 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPDataSource (aka Anteros-DBCP).	8.1	More Details
CVE-2020-14508	GateManager versions prior to 9.2c, The affected product is vulnerable to an off-by-one error, which may allow an attacker to remotely execute arbitrary code or cause a denial-of-service condition.	8.1	More Details
CVE-2020-14512	GateManager versions prior to 9.2c, The affected product uses a weak hash type, which may allow an attacker to view user passwords.	8.1	More Details
CVE-2020-15151	OpenMage LTS before versions 19.4.6 and 20.0.2 allows attackers to circumvent the `fromkey protection` in the Admin Interface and increases the attack surface for Cross Site Request Forgery attacks. This issue is related to Adobe's CVE-2020-9690. It is patched in versions 19.4.6 and 20.0.2.	8.0	More Details
CVE-2020-9715	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9693	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-24574	The client (aka GalaxyClientService.exe) in GOG GALAXY through 2.0.41 (as of 12:58 AM Eastern, 9/26/21) allows local privilege escalation from any authenticated user to SYSTEM by instructing the Windows service to execute arbitrary commands. This occurs because the attacker can inject a DLL into GalaxyClient.exe, defeating the TCP-based "trusted client" protection mechanism.	7.8	More Details
CVE-2020-24567	voidtools Everything before 1.4.1 Beta Nightly 2020-08-18 allows privilege escalation via a Trojan horse urlmon.dll file in the installation directory. NOTE: this is only relevant if low-privileged users can write to the installation directory, which may be considered a site-specific configuration error	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17404	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11191.	7.8	More Details
CVE-2020-17403	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11003.	7.8	More Details
CVE-2020-9701	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9704	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9698	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-16281	The Kommbox component in Rangee GmbH RangeeOS 8.0.4 could allow a local authenticated attacker to escape from the restricted environment and execute arbitrary code due to unrestricted context menus being accessible.	7.8	More Details
CVE-2020-9714	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to privilege escalation .	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9699	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-15777	An issue was discovered in the Maven Extension plugin before 1.6 for Gradle Enterprise. The extension uses a socket connection to send serialized Java objects. Deserialization is not restricted to an allow-list, thus allowing an attacker to achieve code execution via a malicious deserialization gadget chain. The socket is not bound exclusively to localhost. The port this socket is assigned to is randomly selected and is not intentionally exposed to the public (either by design or documentation). This could potentially be used to achieve remote code execution and local privilege escalation.	7.8	More Details
CVE-2020-14356	A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem in versions before 5.7.10 was found in the way when reboot the system. A local user could use this flaw to crash the system or escalate their privileges on the system.	7.8	More Details
CVE-2020-8870	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files from the GetTIFPalette method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9931.	7.8	More Details
CVE-2020-8869	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.916. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9881.	7.8	More Details
CVE-2020-15862	Net-SNMP through 5.8 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.	7.8	More Details
CVE-2020-15861	Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15638	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.2.29539. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the NodeProperties::InferReceiverMapsUnsafe method. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10950.	7.8	More Details
CVE-2020-9700	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-9722	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-4587	IBM Sterling Connect:Direct for UNIX 4.2.0, 4.3.0, 6.0.0, and 6.1.0 is vulnerable to a stack based buffer ovreflow, caused by improper bounds checking. A local attacker could manipulate CD UNIX to obtain root provileges. IBM X-Force ID: 184578.	7.8	More Details
CVE-2020-15630	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PNG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10977.	7.8	More Details
CVE-2020-15629	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.922. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10764.	7.8	More Details
CVE-2020-9724	Adobe Lightroom versions 9.2.0.10 and earlier have an insecure library loading vulnerability. Successful exploitation could lead to privilege escalation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9694	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	7.8	More Details
CVE-2020-15143	In SyliusResourceBundle before versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4, rrequest parameters injected inside an expression evaluated by `symfony/expression-language` package haven't been sanitized properly. This allows the attacker to access any public service by manipulating that request parameter, allowing for Remote Code Execution. This issue has been patched for versions 1.3.14, 1.4.7, 1.5.2 and 1.6.4. Versions prior to 1.3 were not patched.	7.7	More Details
CVE-2020-10126	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not properly validate softare updates for the bunch note acceptor (BNA), enabling an attacker with physical access to internal ATM components to restart the host computer and execute arbitrary code with SYSTEM privileges because while booting, the update process looks for CAB archives on removable media and executes a specific file without first validating the signature of the CAB archive.	7.6	More Details
CVE-2020-10125	NCR SelfServ ATMs running APTRA XFS 04.02.01 and 05.01.00 implement 512-bit RSA certificates to validate bunch note acceptor (BNA) software updates, which can be broken by an attacker with physical access in a sufficiently short period of time, thereby enabling the attacker to sign arbitrary files and CAB archives used to update BNA software, as well as bypass application whitelisting, resulting in the ability to execute arbitrary code.	7.6	More Details
CVE-2020-9063	NCR SelfServ ATMs running APTRA XFS 05.01.00 or earlier do not authenticate or protect the integrity of USB HID communications between the currency dispenser and the host computer, permitting an attacker with physical access to internal ATM components the ability to inject a malicious payload and execute arbitrary code with SYSTEM privileges on the host computer by causing a buffer overflow on the host.	7.6	More Details
CVE-2020-12457	An issue was discovered in wolfSSL before 4.5.0. It mishandles the change_cipher_spec (CCS) message processing logic for TLS 1.3. If an attacker sends ChangeCipherSpec messages in a crafted way involving more than one in a row, the server becomes stuck in the ProcessReply() loop, i.e., a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17385	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly, which allows unauthorized user to launch Path Traversal attack and access arbitrate file on the system.	7.5	More Details
CVE-2020-8623	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker	7.5	More Details
CVE-2020-24053	Moog EXO Series EXVF5C-2 and EXVP7C2-3 units have a hardcoded credentials vulnerability. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols.	7.5	More Details
CVE-2020-7711	This affects all versions of package github.com/russellhaering/goxmldsig. There is a crash on nil-pointer dereference caused by sending malformed XML signatures.	7.5	More Details
CVE-2020-24056	A hardcoded credentials vulnerability exists in Verint 5620PTZ Verint_FW_0_42, Verint 4320 V4320_FW_0_23, V4320_FW_0_31, and Verint S5120FD Verint_FW_0_42units. This could cause a confidentiality issue when using the FTP, Telnet, or SSH protocols.	7.5	More Details
CVE-2020-8621	In BIND 9.14.0 -> 9.16.5, 9.17.0 -> 9.17.3, If a server is configured with both QNAME minimization and 'forward first' then an attacker who can send queries to it may be able to trigger the condition that will cause the server to crash. Servers that 'forward only' are not affected.	7.5	More Details
CVE-2020-8620	In BIND 9.15.6 -> 9.16.5, 9.17.0 -> 9.17.3, An attacker who can establish a TCP connection with the server and send data on that connection can exploit this to trigger the assertion failure, causing the server to exit.	7.5	More Details
CVE-2020-13101	In OASIS Digital Signature Services (DSS) 1.0, an attacker can control the validation outcome (i.e., trigger either a valid or invalid outcome for a valid or invalid signature) via a crafted XML signature, when the InlineXML option is used. This defeats the expectation of non-repudiation.	7.5	More Details
CVE-2020-19878	DBHcms v1.2.0 has a sensitive information leaks vulnerability as there is no security access control in /dbhcms/ext/news/ext.news.be.php, A remote unauthenticated attacker can exploit this vulnerability to get path information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24381	GUnet Open eClass Platform (aka openeclass) before 3.11 might allow remote attackers to read students' submitted assessments because it does not ensure that the web server blocks directory listings, and the data directory is inside the web root by default.	7.5	More Details
CVE-2020-24571	NexusQA NexusDB before 4.50.23 allows the reading of files via ../ directory traversal.	7.5	More Details
CVE-2020-24359	HashiCorp vault-ssh-helper up to and including version 0.1.6 incorrectly accepted Vault-issued SSH OTPs for the subnet in which a host's network interface was located, rather than the specific IP address assigned to that interface. Fixed in 0.2.0.	7.5	More Details
CVE-2020-14522	Softing Industrial Automation all versions prior to the latest build of version 4.47.0, The affected product is vulnerable to uncontrolled resource consumption, which may allow an attacker to cause a denial-of-service condition.	7.5	More Details
CVE-2020-9705	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-11848	Denial of service vulnerability on Micro Focus ArcSight Management Center. Affecting all versions prior to version 2.9.5. The vulnerability could cause the server to become unavailable, causing a denial of service.	7.5	More Details
CVE-2020-24368	Icinga Icinga Web2 2.0.0 through 2.6.4, 2.7.4 and 2.8.2 has a Directory Traversal vulnerability which allows an attacker to access arbitrary files that are readable by the process running Icinga Web 2. This issue is fixed in Icinga Web 2 in v2.6.4, v2.7.4 and v2.8.2.	7.5	More Details
CVE-2020-9716	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-9723	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 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-2020-15640	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getFileUploadBytes method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10497.	7.5	More Details
CVE-2020-9721	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-14215	Zulip Server before 2.1.5 has Incorrect Access Control because 0198_preregistrationuser_invited_as adds the administrator role to invitations.	7.5	More Details
CVE-2020-9717	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-9720	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-9719	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-9718	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-15641	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Marvell QConvergeConsole 5.5.0.64. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getFileUploadBytes method of the FlashValidatorServiceImpl class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-10499.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-11847	An improper privilege management vulnerabitlity exists in ALEOS before 4.11.0, 4.9.4 and 4.4.9. An authenticated user can escalate to root via the command shell.	7.3	More Details
CVE-2020-14350	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23.	7.3	More Details
CVE-2020-17384	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly. With the cookie of the system administrator, attackers can inject and remotely execute arbitrary command to manipulate the system.	7.2	More Details
CVE-2020-19891	DBHcms v1.2.0 has an Arbitrary file write vulnerability in dbhcms\mod\mod.editor.php $_POST['updatefile'] is filename and $_POST['tinymce_content'] is file content, there is no filter function for security. A remote authenticated admin user can exploit this vulnerability to get a webshell.	7.2	More Details
CVE-2020-14044	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** A Server-Side Request Forgery (SSRF) vulnerability was found in Codiad v1.7.8 and later. A user with admin privileges could use the plugin install feature to make the server request any URL via components/market/class.market.php. This could potentially result in remote code execution. NOTE: the vendor states "Codiad is no longer under active maintenance by core contributors."	7.2	More Details
CVE-2020-7376	The Metasploit Framework module "post/osx/gather/enum_osx module" is affected by a relative path traversal vulnerability in the get_keychains method which can be exploited to write arbitrary files to arbitrary locations on the host filesystem when the module is run on a malicious host.	7.1	More Details
CVE-2020-5774	Nessus versions 8.11.0 and earlier were found to maintain sessions longer than the permitted period in certain scenarios. The lack of proper session expiration could allow attackers with local access to login into an existing browser session.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7705	This affects the package MintegralAdSDK from 0.0.0. The SDK distributed by the company contains malicious functionality that tracks any URL opened by the app and reports it back to the company, along with performing advertisement attribution fraud. Mintegral can remotely activate hooks on the UIApplication, openURL, SKStoreProductViewController, loadProductWithParameters and NSURLProtocol methods along with anti-debug and proxy detection protection. If those hooks are active MintegralAdSDK sends obfuscated data about every opened URL in an application to their servers. Note that the malicious functionality is enabled even if the SDK was not enabled to serve ads.	7.1	More Details
CVE-2020-14349	It was found that PostgreSQL versions before 12.4, before 11.9 and before 10.14 did not properly sanitize the search_path during logical replication. An authenticated attacker could use this flaw in an attack similar to CVE-2018-1058, in order to execute arbitrary SQL command in the context of the user used for replication.	7.1	More Details
CVE-2020-24394	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.	7.1	More Details
CVE-2020-10124	NCR SelfServ ATMs running APTRA XFS 05.01.00 do not encrypt, authenticate, or verify the integrity of messages between the BNA and the host computer, which could allow an attacker with physical access to the internal components of the ATM to execute arbitrary code, including code that enables the attacker to commit deposit forgery.	7.1	More Details
CVE-2020-15309	An issue was discovered in wolfSSL before 4.5.0, when single precision is not employed. Local attackers can conduct a cache-timing attack against public key operations. These attackers may already have obtained sensitive information if the affected system has been used for private key operations (e.g., signing with a private key).	7.0	More Details
CVE-2020-7310	Privilege Escalation vulnerability in the installer in McAfee McAfee Total Protection (MTP) trial prior to 4.0.161.1 allows local users to change files that are part of write protection rules via manipulating symbolic links to redirect a McAfee file operations to an unintended file.	6.9	More Details
CVE-2020-10290	Universal Robots controller execute URCaps (zip files containing Java-powered applications) without any permission restrictions and a wide API that presents many primitives that can compromise the overall robot operations as demonstrated in our video. In our PoC we demonstrate how a malicious actor could 'cook' a custom URCap that when deployed by the user (intendedly or unintendedly) compromises the system	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-24613	wolfSSL before 4.5.0 mishandles TLS 1.3 server data in the WAIT_CERT_CR state, within SanityCheckTls13MsgReceived() in tls13.c. This is an incorrect implementation of the TLS 1.3 client state machine. This allows attackers in a privileged network position to completely impersonate any TLS 1.3 servers, and read or modify potentially sensitive information between clients using the wolfSSL library and these TLS servers.	6.8	More Details
CVE-2020-8227	Missing sanitization of a server response in Nextcloud Desktop Client 2.6.4 for Linux allowed a malicious Nextcloud Server to store files outside of the dedicated sync directory.	6.8	More Details
CVE-2020-24612	An issue was discovered in the selinux-policy (aka Reference Policy) package 3.14 through 2020-08-24 because the .config/Yubico directory is mishandled. Consequently, when SELinux is in enforced mode, pam-u2f is not allowed to read the user's U2F configuration file. If configured with the nouserok option (the default when configured by the authselect tool), and that file cannot be read, the second factor is disabled. An attacker with only the knowledge of the password can then log in, bypassing 2FA.	6.7	More Details
CVE-2020-4381	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.6 could allow an authenticated user to cause a denial of service during deployment or upgrade if GUI specific services are enabled. IBM X-Force ID: 179162.	6.5	More Details
CVE-2020-4648	A vulnerability exsists in IBM Planning Analytics 2.0 whereby avatars in Planning Analytics Workspace could be modified by other users without authorization to do so. IBM X-Force ID: 186019.	6.5	More Details
CVE-2020-8622	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of the packet and message, and spoof a truncated response to trigger an assertion failure, causing the server to exit.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17402	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4 (47270). An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. By examining a log file, an attacker can disclose a memory address. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-11063.	6.5	More Details
CVE-2020-17386	Cellopoint Cellos v4.1.10 Build 20190922 does not validate URL inputted properly. With cookie of an authenticated user, attackers can temper with the URL parameter and access arbitrary file on system.	6.5	More Details
CVE-2020-17398	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-11302.	6.5	More Details
CVE-2020-7824	A vulnerability in the web-based management interface of iPECS could allow an authenticated, remote attacker to get administrator permission. The vulnerability is due to insecure permission when handling session cookies. An attacker could exploit this vulnerability by modification the cookie value to an affected device. A successful exploit could allow the attacker access to sensitive device information, which includes configuration files.	6.5	More Details
CVE-2020-9246	FusionCompute 8.0.0 has an information leak vulnerability. A module does not launch strict access control and information protection. Attackers with low privilege can get some extra information. This can lead to information leak.	6.5	More Details
CVE-2020-23574	When uploading a file in Sysax Multi Server 6.90, an authenticated user can modify the filename="" parameter in the uploadfile_name1.htm form to a length of 368 or more bytes. This will create a buffer overflow condition, causing the application to crash.	6.5	More Details
CVE-2020-20634	Elementor 2.9.5 and below WordPress plugin allows authenticated users to activate its safe mode feature. This can be exploited to disable all security plugins on the blog.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4383	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment while configuring some of the network services. IBM X-Force ID: 179165.	6.5	More Details
CVE-2020-24591	The Management Console in certain WSO2 products allows XXE attacks during EventReceiver updates. This affects API Manager through 3.0.0, API Manager Analytics 2.2.0 and 2.5.0, API Microgateway 2.2.0, Enterprise Integrator 6.2.0 and 6.3.0, and Identity Server Analytics through 5.6.0.	6.5	More Details
CVE-2020-14201	Dolibarr CRM before 11.0.5 allows privilege escalation. This could allow remote authenticated attackers to upload arbitrary files via societe/document.php in which "disabled" is changed to "enabled" in the HTML source code.	6.5	More Details
CVE-2020-7923	A user authorized to perform database queries may cause denial of service by issuing specially crafted queries, which violate an invariant in the query subsystem's support for geoNear. This issue affects MongoDB Server v4.4 versions prior to 4.4.0-rc7; MongoDB Server v4.2 versions prior to 4.2.8 and MongoDB Server v4.0 versions prior to 4.0.19.	6.5	More Details
CVE-2020-17391	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.3-47255. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handler for HOST_IOCTL_INIT_HYPERVISOR in the prl_hypervisor kext. The issue results from the exposure of dangerous method or function to the unprivileged user. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-10518.	6.5	More Details
CVE-2019-20150	In TreasuryXpress 19191105, a logged-in user can discover saved credentials, even though the UI hides them. Using functionality within the application and a malicious host, it is possible to force the application to expose saved SSH/SFTP credentials. This can be done by using the application's editor to change the expected SFTP Host IP to a malicious host, and then using the Check Connectivity option. The application then sends these saved credentials to the malicious host.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-17393	This vulnerability allows local attackers to disclose information on affected installations of Parallels Desktop 15.1.3-47255. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the prl_hypervisor kext. The issue results from the lack of proper validation of user-supplied data, which can result a pointer to be leaked after the handler is done. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-10520.	6.5	More Details
CVE-2020-15532	Silicon Labs Bluetooth Low Energy SDK before 2.13.3 has a buffer overflow via packet data. This is an over-the-air denial of service vulnerability in Bluetooth LE in EFR32 SoCs and associated modules running Bluetooth SDK, supporting Central or Observer roles.	6.5	More Details
CVE-2020-5416	Cloud Foundry Routing (Gorouter), versions prior to 0.204.0, when used in a deployment with NGINX reverse proxies in front of the Gorouters, is potentially vulnerable to denial-of-service attacks in which an unauthenticated malicious attacker can send specially-crafted HTTP requests that may cause the Gorouters to be dropped from the NGINX backend pool.	6.5	More Details
CVE-2020-15119	In auth0-lock versions before and including 11.25.1, dangerouslySetInnerHTML is used to update the DOM. When dangerouslySetInnerHTML is used, the application and its users might be exposed to cross-site scripting (XSS) attacks.	6.4	More Details
CVE-2019-11850	A stack overflow vulnerabiltity exist in the AT command interface of ALEOS before 4.11.0. The vulnerability may allow code execution	6.3	More Details
CVE-2019-11849	A stack overflow vulnerabiltity exists in the AT command APIs of ALEOS before 4.11.0. The vulnerability may allow code execution.	6.3	More Details
CVE-2020-15634	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9755.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15858	Some devices of Thales DIS (formerly Gemalto, formerly Cinterion) allow Directory Traversal by physically proximate attackers. The directory path access check of the internal flash file system can be circumvented. This flash file system can store application-specific data and data needed for customer Java applications, TLS and OTAP (Java over-the-air-provisioning) functionality. The affected products and releases are: BGS5 up to and including SW RN 02.000 / ARN 01.001.06 EHSx and PDSx up to and including SW RN 04.003 / ARN 01.000.04 ELS61 up to and including SW RN 02.002 / ARN 01.000.04 ELS81 up to and including SW RN 05.002 / ARN 01.000.04 PLS62 up to and including SW RN 02.000 / ARN 01.000.04	6.2	More Details
CVE-2019-20151	An XSS issue was discovered in TreasuryXpress 19191105. Due to the lack of filtering and sanitization of user input, malicious JavaScript can be executed by the application's administrator(s). A malicious payload can be injected within the Multi Approval security component and inserted via the Note field. As a result, the payload is executed by the application's administrator(s).	6.1	More Details
CVE-2020-13825	A cross-site scripting (XSS) vulnerability in i-doit 1.14.2 allows remote attackers to inject arbitrary web script or HTML via the viewMode, tvMode, tvType, objID, catgID, objTypeID, or editMode parameter.	6.1	More Details
CVE-2020-4598	IBM Security Guardium Insights 2.0.1 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 184823.	6.1	More Details
CVE-2020-14042	** PRODUCT NOT SUPPORTED WHEN ASSIGNED ** A Cross Site Scripting (XSS) vulnerability was found in Codiad v1.7.8 and later. The vulnerability occurs because of improper sanitization of the folder's name $path variable in components/filemanager/class.filemanager.php. NOTE: the vendor states "Codiad is no longer under active maintenance by core contributors."	6.1	More Details
CVE-2020-24609	TechKshetra Info Solutions Pvt. Ltd Savsoft Quiz 5.5 and earlier has XSS which can result in an attacker injecting the XSS payload in the User Registration section and each time the admin visits the manage user section from the admin panel, the XSS triggers and the attacker can steal the cookie via crafted payload.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-12759	Zulip Server before 2.1.5 allows reflected XSS via the Dropbox webhook.	6.1	More Details
CVE-2019-20152	An XSS issue was discovered in TreasuryXpress 19191105. Due to the lack of filtering and sanitization of user input, malicious JavaScript can be executed throughout the application. A malicious payload can be injected within the Custom Workflow component and inserted via the Create New Workflow field. As a result, the payload is executed via the navigation bar throughout the application.	6.1	More Details
CVE-2020-5540	Cross-site scripting vulnerability in CyberMail Ver.6.x and Ver.7.x allows remote attackers to inject arbitrary script or HTML via a specially crafted URL.	6.1	More Details
CVE-2020-5541	Open redirect vulnerability in CyberMail Ver.6.x and Ver.7.x allows remote attackers to redirect users to arbitrary sites and conduct phishing attacks via a specially crafted URL.	6.1	More Details
CVE-2020-4653	IBM Planning Analytics 2.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	6.1	More Details
CVE-2020-19880	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function form 'Name' in dbhcms\types.php, A remote unauthenticated attacker can exploit this vulnerability to hijack other users.	6.1	More Details
CVE-2020-19879	DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter of $_GET['dbhcms_pid'] variable in dbhcms\page.php line 107,	6.1	More Details
CVE-2020-17401	This vulnerability allows local attackers to disclose sensitive informations on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the VGA virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated array. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11363.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14367	A flaw was found in chrony versions before 3.5.1 when creating the PID file under the /var/run/chrony folder. The file is created during chronyd startup while still running as the root user, and when it's opened for writing, chronyd does not check for an existing symbolic link with the same file name. This flaw allows an attacker with privileged access to create a symlink with the default PID file name pointing to any destination file in the system, resulting in data loss and a denial of service due to the path traversal.	6.0	More Details
CVE-2019-11859	A buffer overflow exists in the SMS handler API of ALEOS before 4.13.0, 4.9.5, 4.9.4 that may allow code execution as root.	6.0	More Details
CVE-2020-17394	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the OEMNet component. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute code in the context of the hypervisor. Was ZDI-CAN-11132.	6.0	More Details
CVE-2020-19888	DBHcms v1.2.0 has an unauthorized operation vulnerability because there's no access control at line 175 of dbhcms\page.php for empty cache operation. This vulnerability can be exploited to empty a table.	5.9	More Details
CVE-2020-12619	MailMate before 1.11 automatically imported S/MIME certificates and thereby silently replaced existing ones. This allowed a man-in-the-middle attacker to obtain an email-validated S/MIME certificate from a trusted CA and replace the public key of the entity to be impersonated. This enabled the attacker to decipher further communication. The entire attack could be accomplished by sending a single email.	5.9	More Details
CVE-2020-5775	Server-Side Request Forgery in Canvas LMS 2020-07-29 allows a remote, unauthenticated attacker to cause the Canvas application to perform HTTP GET requests to arbitrary domains.	5.8	More Details
CVE-2020-19005	zrlog v2.1.0 has a vulnerability with the permission check. If admin account is logged in, other unauthorized users can download the database backup file directly.	5.7	More Details
CVE-2019-11858	Multiple buffer overflow vulnerabilities exist in the AceManager Web API of ALEOS before 4.13.0, 4.9.5, and 4.4.9.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9096	HUAWEI P30 Pro smartphones with Versions earlier than 10.1.0.160(C00E160R2P8) have an out of bound read vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause out-of-bound read. This can compromise normal service.	5.5	More Details
CVE-2020-9095	HUAWEI P30 Pro smartphone with Versions earlier than 10.1.0.160(C00E160R2P8) has an integer overflow vulnerability. Some functions are lack of verification when they process some messages sent from other module. Attackers can exploit this vulnerability by send malicious message to cause integer overflow. This can compromise normal service.	5.5	More Details
CVE-2020-24240	GNU Bison before 3.7.1 has a use-after-free in _obstack_free in lib/obstack.c (called from gram_lex) when a '\0' byte is encountered. NOTE: there is a risk only if Bison is used with untrusted input, and the observed bug happens to cause unsafe behavior with a specific compiler/architecture. The bug report was intended to show that a crash may occur in Bison itself, not that a crash may occur in code that is generated by Bison.	5.5	More Details
CVE-2020-9712	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	5.5	More Details
CVE-2020-24241	In Netwide Assembler (NASM) 2.15rc10, there is heap use-after-free in saa_wbytes in nasmlib/saa.c.	5.5	More Details
CVE-2020-16280	Multiple Rangee GmbH RangeeOS 8.0.4 modules store credentials in plaintext including credentials of users for several external facing administrative services, domain joined users, and local administrators. To exploit the vulnerability a local attacker must have access to the underlying operating system.	5.5	More Details
CVE-2020-9696	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	5.5	More Details
CVE-2020-4382	IBM Spectrum Scale for IBM Elastic Storage Server 5.3.0 through 5.3.5 could allow an authenticated user to cause a denial of service during deployment or upgrade pertaining to xcat services. IBM X-Force ID: 179163.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9702	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service.	5.5	More Details
CVE-2020-9703	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service.	5.5	More Details
CVE-2020-9697	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have a disclosure of sensitive data vulnerability. Successful exploitation could lead to memory leak.	5.5	More Details
CVE-2020-24242	In Netwide Assembler (NASM) 2.15rc10, SEGV can be triggered in tok_text in asm/preproc.c by accessing READ memory.	5.5	More Details
CVE-2020-14194	Zulip Server before 2.1.5 allows reverse tabnapping via a topic header link.	5.4	More Details
CVE-2020-20633	ajax_policy_generator in admin/modules/cli-policy-generator/classes/class-policy-generator-ajax.php in GDPR Cookie Consent (cookie-law-info) 1.8.2 and below plugin for WordPress, allows authenticated stored XSS and privilege escalation.	5.4	More Details
CVE-2020-5620	Cross-site scripting vulnerability in Exment prior to v3.6.0 allows remote authenticated attackers to inject arbitrary script or HTML via a specially crafted file.	5.4	More Details
CVE-2020-5619	Cross-site scripting vulnerability in Exment prior to v3.6.0 allows remote authenticated attackers to inject arbitrary script or HTML via unspecified vectors.	5.4	More Details
CVE-2020-8189	A cross-site scripting error in Nextcloud Desktop client 2.6.4 allowed to present any html (including local links) when responding with invalid data on the login attempt.	5.4	More Details
CVE-2020-4165	IBM Security Guardium Insights 2.0.1 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: 174401.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3975	VMware App Volumes 2.x prior to 2.18.6 and VMware App Volumes 4 prior to 2006 contain a Stored Cross-Site Scripting (XSS) vulnerability. A malicious actor with access to create and edit applications or create storage groups, may be able to inject malicious script which will be executed by a victim's browser when viewing.	5.4	More Details
CVE-2020-9062	Diebold Nixdorf ProCash 2100xe USB ATMs running Wincor Probase version 1.1.30 do not encrypt, authenticate, or verify the integrity of messages between the CCDM and the host computer, allowing an attacker with physical access to internal ATM components to commit deposit forgery by intercepting and modifying messages to the host computer, such as the amount and value of currency being deposited.	5.3	More Details
CVE-2020-10123	The currency dispenser of NCR SelfSev ATMs running APTRA XFS 05.01.00 or earlier does not adequately authenticate session key generation requests from the host computer, allowing an attacker with physical access to internal ATM components to issue valid commands to dispense currency by generating a new session key that the attacker knows.	5.3	More Details
CVE-2020-19877	DBHcms v1.2.0 has a directory traversal vulnerability as there is no directory control function in directory /dbhcms/. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	5.3	More Details
CVE-2020-14518	Philips DreamMapper, Version 2.24 and prior. Information written to log files can give guidance to a potential attacker.	5.3	More Details
CVE-2020-24585	An issue was discovered in the DTLS handshake implementation in wolfSSL before 4.5.0. Clear DTLS application_data messages in epoch 0 do not produce an out-of-order error. Instead, these messages are returned to the application.	5.3	More Details
CVE-2020-3976	VMware ESXi and vCenter Server contain a partial denial of service vulnerability in their respective authentication services. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.3.	5.3	More Details
CVE-2020-10775	An Open redirect vulnerability was found in ovirt-engine versions 4.4 and earlier, where it allows remote attackers to redirect users to arbitrary web sites and attempt phishing attacks. Once the target has opened the malicious URL in their browser, the critical part of the URL is no longer visible. The highest threat from this vulnerability is on confidentiality.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19890	DBHcms v1.2.0 has an Arbitrary file read vulnerability in dbhcms\mod\mod.editor.php $_GET['file'] is filename,and as there is no filter function for security, you can read any file's content.	4.9	More Details
CVE-2020-24622	In Sonatype Nexus Repository 3.26.1, an S3 secret key can be exposed by an admin user.	4.9	More Details
CVE-2020-16239	Philips SureSigns VS4, A.07.107 and prior. When an actor claims to have a given identity, the software does not prove or insufficiently proves the claim is correct.	4.9	More Details
CVE-2020-19885	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_name']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	4.8	More Details
CVE-2020-19887	DBHcms v1.2.0 has a stored XSS vulnerability as there is no htmlspecialchars function for '$_POST['pageparam_insert_description']' variable in dbhcms\mod\mod.page.edit.php line 227, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	4.8	More Details
CVE-2020-12618	eM Client before 7.2.33412.0 automatically imported S/MIME certificates and thereby silently replaced existing ones. This allowed a man-in-the-middle attacker to obtain an email-validated S/MIME certificate from a trusted CA and replace the public key of the entity to be impersonated. This enabled the attacker to decipher further communication. The entire attack could be accomplished by sending a single email.	4.8	More Details
CVE-2020-19884	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function in dbhcms\mod\mod.domain.edit.php line 119.	4.8	More Details
CVE-2020-19883	DBHcms v1.2.0 has a stored xss vulnerability as there is no security filter in dbhcms\mod\mod.users.view.php line 57 for user_login, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	4.8	More Details
CVE-2020-19882	DBHcms v1.2.0 has a stored xss vulnerability as there is no htmlspecialchars function for 'menu_description' variable in dbhcms\mod\mod.menus.edit.php line 83 and in dbhcms\mod\mod.menus.view.php line 111, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19881	DBHcms v1.2.0 has a reflected xss vulnerability as there is no security filter in dbhcms\mod\mod.selector.php line 108 for $_GET['return_name'] parameter, A remote authenticated with admin user can exploit this vulnerability to hijack other users.	4.8	More Details
CVE-2018-1985	IBM Trusteer Rapport/Apex 3.6.1908.22 contains an unused legacy driver which could allow a user with administrator privileges to cause a buffer overflow that would result in a kernel panic. IBM X-Force ID: 154207.	4.4	More Details
CVE-2020-4593	IBM Security Guardium Insights 2.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 184747.	4.4	More Details
CVE-2020-4170	IBM Security Guardium Insights 2.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 174406.	4.3	More Details
CVE-2020-4687	IBM Content Navigator 3.0.7 and 3.0.8 could allow an authenticated user to view cached content of another user that they should not have access to. IBM X-Force ID: 186679.	4.3	More Details
CVE-2020-16197	An issue was discovered in Octopus Deploy 3.4. A deployment target can be configured with an Account or Certificate that is outside the scope of the deployment target. An authorised user can potentially use a certificate that they are not in scope to use. An authorised user is also able to obtain certificate metadata by associating a certificate with certain resources that should fail scope validation.	4.3	More Details
CVE-2020-9104	HUAWEI P30 smartphones with Versions earlier than 10.1.0.123(C431E22R2P5),Versions earlier than 10.1.0.123(C432E22R2P5),Versions earlier than 10.1.0.126(C10E7R5P1),Versions earlier than 10.1.0.126(C185E4R7P1),Versions earlier than 10.1.0.126(C461E7R3P1),Versions earlier than 10.1.0.126(C605E19R1P3),Versions earlier than 10.1.0.126(C636E7R3P4),Versions earlier than 10.1.0.128(C635E3R2P4),Versions earlier than 10.1.0.160(C00E160R2P11),Versions earlier than 10.1.0.160(C01E160R2P11) have a denial of service vulnerability. In specific scenario, due to the improper resource management and memory leak of some feature, the attacker could exploit this vulnerability to cause the device reset.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8624	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone.	4.3	More Details
CVE-2019-11848	An API abuse vulnerability exists in the AT command API of ALEOS before 4.13.0, 4.9.5, 4.4.9 due to lack of length checking when handling certain user-provided values.	4.1	More Details
CVE-2019-11853	Several potential command injections vulnerabilities exist in the AT command interface of ALEOS before 4.11.0, and 4.9.4.	3.9	More Details
CVE-2019-11852	An out-of-bounds reads vulnerability exists in the ACEView Service of ALEOS before 4.13.0, 4.9.5, and 4.4.9. Sensitive information may be disclosed via the ACEviewservice, accessible by default on the LAN.	3.7	More Details
CVE-2020-9710	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	3.3	More Details
CVE-2019-11856	A nonce reuse vulnerability exists in the ACEView service of ALEOS before 4.13.0, 4.9.5, and 4.4.9 allowing message replay. Captured traffic to the ACEView service can be replayed to other gateways sharing the same credentials.	3.3	More Details
CVE-2020-9706	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	3.3	More Details
CVE-2020-9707	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-15637	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the SetLocalDescription method. By performing actions in JavaScript, an attacker can cause a pointer to be reused after it has been freed. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10972.	3.3	More Details
CVE-2020-4548	IBM Content Navigator 3.0.7 and 3.0.8 is vulnerable to improper input validation. A malicious administrator could bypass the user interface and send requests to the IBM Content Navigator server with illegal characters that could be stored in the IBM Content Navigator database. IBM X-Force ID: 183316.	2.7	More Details
CVE-2020-16241	Philips SureSigns VS4, A.07.107 and prior. The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor.	2.1	More Details
CVE-2020-16237	Philips SureSigns VS4, A.07.107 and prior. The product receives input or data, but it does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly.	2.1	More Details
CVE-2019-19184	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-2019-19120	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-2020-14357	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-2019-19183	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-2019-19181	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-19179	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-2019-19178	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-2019-19173	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-2019-19123	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-2019-19121	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