SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 April 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-2020-3936	UltraLog Express device management interface does not properly filter user inputted string in some specific parameters, attackers can inject arbitrary SQL command.	10.0	More Details
CVE-2020-5553	mailform version 1.04 allows remote attackers to execute arbitrary PHP code via unspecified vectors.	9.8	More Details
CVE-2015-5684	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A buffer overflow vulnerability was reported, (fixed and publicly disclosed in 2015) in the Lenovo Service Engine (LSE), affecting various versions of BIOS for Lenovo Notebooks, that could allow a remote user to execute arbitrary code on the system.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-6815	Mozilla developers reported memory safety and script safety bugs present in Firefox 73. Some of these bugs showed evidence of memory corruption or escalation of privilege and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 74.	9.8	More Details
CVE-2020-10245	CODESYS V3 web server before 3.5.15.40, as used in CODESYS Control runtime systems, has a buffer overflow.	9.8	More Details
CVE-2020-10823	A stack-based buffer overflow in /cgi-bin/activate.cgi through var parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 1 of 3).	9.8	More Details
CVE-2020-10824	A stack-based buffer overflow in /cgi-bin/activate.cgi through ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 2 of 3).	9.8	More Details
CVE-2020-10825	A stack-based buffer overflow in /cgi-bin/activate.cgi while base64 decoding ticket parameter on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request (issue 3 of 3).	9.8	More Details
CVE-2020-10826	/cgi-bin/activate.cgi on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve command injection via a remote HTTP request in DEBUG mode.	9.8	More Details
CVE-2020-10827	A stack-based buffer overflow in apmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request.	9.8	More Details
CVE-2020-10828	A stack-based buffer overflow in cvmd on Draytek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1 allows remote attackers to achieve code execution via a remote HTTP request.	9.8	More Details
CVE-2020-10990	An XXE issue exists in Accenture Mercury before 1.12.28 because of the platformlambda/core/serializers/SimpleXmlParser.java component.	9.8	More Details
CVE-2020-10991	Mulesoft APIkit through 1.3.0 allows XXE because of validation/RestXmlSchemaValidator.java	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10992	Azkaban through 3.84.0 allows XXE, related to validator/XmlValidatorManager.java and user/XmlUserManager.java.	9.8	More Details
CVE-2020-10956	GitLab 8.10 and later through 12.9 is vulnerable to an SSRF in a project import note feature.	9.8	More Details
CVE-2020-3789	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-7610	All versions of bson before 1.1.4 are vulnerable to Deserialization of Untrusted Data. The package will ignore an unknown value for an object's _bsotype, leading to cases where an object is serialized as a document rather than the intended BSON type.	9.8	More Details
CVE-2016-11023	odata4j 0.7.0 allows ExecuteCountQueryCommand.java SQL injection. NOTE: this product is apparently discontinued.	9.8	More Details
CVE-2016-11024	odata4j 0.7.0 allows ExecuteJPQLQueryCommand.java SQL injection. NOTE: this product is apparently discontinued.	9.8	More Details
CVE-2020-5723	The UCM6200 series 1.0.20.22 and below stores unencrypted user passwords in an SQLite database. This could allow an attacker to retrieve all passwords and possibly gain elevated privileges.	9.8	More Details
CVE-2019-19605	X-Plane before 11.41 allows Arbitrary Memory Write via crafted network packets, which could cause a denial of service or arbitrary code execution.	9.8	More Details
CVE-2019-19606	X-Plane before 11.41 has multiple improper path validations that could allow reading and writing files from/to arbitrary paths (or a leak of OS credentials to a remote system) via crafted network packets. This could be used to execute arbitrary commands on the system.	9.8	More Details
CVE-2020-10374	A webserver component in Paessler PRTG Network Monitor 19.2.50 to PRTG 20.1.56 allows unauthenticated remote command execution via a crafted POST request or the what parameter of the screenshot function in the Contact Support form.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11105	An issue was discovered in USC iLab cereal through 1.3.0. It employs caching of std::shared_ptr values, using the raw pointer address as a unique identifier. This becomes problematic if an std::shared_ptr variable goes out of scope and is freed, and a new std::shared_ptr is allocated at the same address. Serialization fidelity thereby becomes dependent upon memory layout. In short, serialized std::shared_ptr variables cannot always be expected to serialize back into their original values. This can have any number of consequences, depending on the context within which this manifests.	9.8	More Details
CVE-2020-7611	All versions of io.micronaut:micronaut-http-client before 1.2.11 and all versions from 1.3.0 before 1.3.2 are vulnerable to HTTP Request Header Injection due to not validating request headers passed to the client.	9.8	More Details
CVE-2020-10595	pam-krb5 before 4.9 has a buffer overflow that might cause remote code execution in situations involving supplemental prompting by a Kerberos library. It may overflow a buffer provided by the underlying Kerberos library by a single '\0' byte if an attacker responds to a prompt with an answer of a carefully chosen length. The effect may range from heap corruption to stack corruption depending on the structure of the underlying Kerberos library, with unknown effects but possibly including code execution. This code path is not used for normal authentication, but only when the Kerberos library does supplemental prompting, such as with PKINIT or when using the non-standard no_prompt PAM configuration option.	9.8	More Details
CVE-2020-4208	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174975.	9.8	More Details
CVE-2020-6008	LifterLMS Wordpress plugin version below 3.37.15 is vulnerable to arbitrary file write leading to remote code execution	9.8	More Details
CVE-2020-6814	Mozilla developers reported memory safety bugs present in Firefox and Thunderbird 68.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.	9.8	More Details
CVE-2020-10964	Serendipity before 2.3.4 on Windows allows remote attackers to execute arbitrary code because the filename of a renamed file may end with a dot. This file may then be renamed to have a .php filename.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3788	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-3807	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-5556	Shihonkanri Plus GOOUT Ver1.5.8 and Ver2.2.10 allows remote attackers to execute arbitrary OS commands via unspecified vectors.	9.8	More Details
CVE-2020-5560	WL-Enq 1.11 and 1.12 allows remote attackers to execute arbitrary OS commands with the administrative privilege via unspecified vectors.	9.8	More Details
CVE-2020-5561	Keijiban Tsumiki v1.15 allows remote attackers to execute arbitrary OS commands via unspecified vectors.	9.8	More Details
CVE-2020-10789	openITCOCKPIT before 3.7.3 has a web-based terminal that allows attackers to execute arbitrary OS commands via shell metacharacters that are mishandled on an su command line in app/Lib/SudoMessageInterface.php.	9.8	More Details
CVE-2020-1957	Apache Shiro before 1.5.2, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass.	9.8	More Details
CVE-2020-3792	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-3793	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3795	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-3797	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-3799	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-3801	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-3805	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	9.8	More Details
CVE-2020-3775	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-3785	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-10881	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of DNS responses. A crafted DNS message can trigger an overflow of a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the root user. Was ZDI-CAN-9660.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3787	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-10885	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of DNS responses. The issue results from the lack of proper validation of DNS reponses prior to further processing. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the root user. Was ZDI-CAN-9661.	9.8	More Details
CVE-2020-10886	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the tmpServer service, which listens on TCP port 20002. 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 the current process. Was ZDI-CAN-9662.	9.8	More Details
CVE-2020-10887	This vulnerability allows a firewall bypass on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of IPv6 connections. The issue results from the lack of proper filtering of IPv6 SSH connections. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9663.	9.8	More Details
CVE-2020-10888	This vulnerability allows remote attackers to bypass authentication on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of SSH port forwarding requests during initial setup. The issue results from the lack of proper authentication prior to establishing SSH port forwarding rules. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the WAN interface. Was ZDI-CAN-9664.	9.8	More Details
CVE-2020-3794	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a file inclusion vulnerability. Successful exploitation could lead to arbitrary code execution of files located in the webroot or its subdirectory.	9.8	More Details
CVE-2020-3783	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a heap corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3786	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-3784	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	9.8	More Details
CVE-2020-5555	Shihonkanri Plus GOOUT Ver1.5.8 and Ver2.2.10 allows remote attackers to read and write data of the files placed in the same directory where it is placed via unspecified vector due to the improper input validation issue.	9.1	More Details
CVE-2020-10993	Osmand through 2.0.0 allow XXE because of binary/BinaryMapIndexReader.java.	9.1	More Details
CVE-2020-10788	openITCOCKPIT before 3.7.3 uses the 1fea123e07f730f76e661bced33a94152378611e API key rather than generating a random API Key for WebSocket connections.	9.1	More Details
CVE-2019-17560	The "Apache NetBeans" autoupdate system does not validate SSL certificates and hostnames for https based downloads. This allows an attacker to intercept downloads of autoupdates and modify the download, potentially injecting malicious code. “Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	9.1	More Details
CVE-2020-5554	Directory traversal vulnerability in Shihonkanri Plus GOOUT Ver1.5.8 and Ver2.2.10 allows remote attackers to read and write arbitrary files via unspecified vectors.	9.1	More Details
CVE-2019-14880	A vulnerability was found in Moodle versions 3.7 before 3.7.3, 3.6 before 3.6.7, 3.5 before 3.5.9 and earlier. OAuth 2 providers who do not verify users' email address changes require additional verification during sign-up to reduce the risk of account compromise.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-6805	When removing data about an origin whose tab was recently closed, a use-after-free could occur in the Quota manager, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2166	Jenkins Pipeline: AWS Steps Plugin 1.40 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-2168	Jenkins Azure Container Service Plugin 1.0.1 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-3773	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-4206	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to execute arbitrary commands on the system in the context of root user, caused by improper validation of user-supplied input. IBM X-Force ID: 174966.	8.8	More Details
CVE-2020-2171	Jenkins RapidDeploy Plugin 4.2 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.8	More Details
CVE-2020-3772	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-3790	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-3802	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	8.8	More Details
CVE-2020-10969	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to javax.swing.JEditorPane.	8.8	More Details
CVE-2020-10968	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.aoju.bus.proxy.provider.remoting.RmiProvider (aka bus-proxy).	8.8	More Details
CVE-2020-10817	The custom-searchable-data-entry-system (aka Custom Searchable Data Entry System) plugin through 1.7.1 for WordPress allows SQL Injection. NOTE: this product is discontinued.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11113	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.openjpa.ee.WASRegistryManagedRuntime (aka openjpa).	8.8	More Details
CVE-2020-11112	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.proxy.provider.remoting.RmiProvider (aka apache/commons-proxy).	8.8	More Details
CVE-2020-3770	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-10884	This vulnerability allows network-adjacent attackers execute arbitrary code on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the tdpServer service, which listens on UDP port 20002 by default. This issue results from the use of hard-coded encryption key. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9652.	8.8	More Details
CVE-2020-11111	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.activemq.* (aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).	8.8	More Details
CVE-2020-5551	Toyota 2017 Model Year DCU (Display Control Unit) allows an unauthenticated attacker within Bluetooth range to cause a denial of service attack and/or execute an arbitrary command. The affected DCUs are installed in Lexus (LC, LS, NX, RC, RC F), TOYOTA CAMRY, and TOYOTA SIENNA manufactured in the regions other than Japan from Oct. 2016 to Oct. 2019. An attacker with certain knowledge on the target vehicle control system may be able to send some diagnostic commands to ECUs with some limited availability impacts; the vendor states critical vehicle controls such as driving, turning, and stopping are not affected.	8.8	More Details
CVE-2020-6811	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as Curl' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.	8.8	More Details
CVE-2019-7755	In webERP 4.15, the Import Bank Transactions function fails to sanitize the content of imported MT940 bank statement files, resulting in the execution of arbitrary SQL queries, aka SQL Injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-2167	Jenkins OpenShift Pipeline Plugin 1.0.56 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	8.8	More Details
CVE-2020-9521	An SQL injection vulnerability was discovered in Micro Focus Service Manager Automation (SMA), affecting versions 2019.08, 2019.05, 2019.02, 2018.08, 2018.05, 2018.02. The vulnerability could allow for the improper neutralization of special elements in SQL commands and may lead to the product being vulnerable to SQL injection.	8.8	More Details
CVE-2020-4237	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 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: 175410.	8.8	More Details
CVE-2020-10696	A path traversal flaw was found in Buildah in versions before 1.14.5. This flaw allows an attacker to trick a user into building a malicious container image hosted on an HTTP(s) server and then write files to the user's system anywhere that the user has permissions.	8.8	More Details
CVE-2020-5558	CuteNews 2.0.1 allows remote authenticated attackers to execute arbitrary PHP code via unspecified vectors.	8.8	More Details
CVE-2020-7009	Elasticsearch versions from 6.7.0 before 6.8.8 and 7.0.0 before 7.6.2 contain a privilege escalation flaw if an attacker is able to create API keys. An attacker who is able to generate an API key can perform a series of steps that result in an API key being generated with elevated privileges.	8.8	More Details
CVE-2020-10607	In Advantech WebAccess, Versions 8.4.2 and prior. A stack-based buffer overflow vulnerability caused by a lack of proper validation of the length of user-supplied data may allow remote code execution.	8.8	More Details
CVE-2020-3780	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-3779	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-6806	By carefully crafting promise resolutions, it was possible to cause an out-of-bounds read off the end of an array resized during script execution. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-8536	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow cross-site request forgery.	8.8	More Details
CVE-2020-6807	When a device was changed while a stream was about to be destroyed, the <code>stream-reinit</code> task may have been executed after the stream was destroyed, causing a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.	8.8	More Details
CVE-2020-3776	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-3774	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution.	8.8	More Details
CVE-2020-2160	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier uses different representations of request URL paths, which allows attackers to craft URLs that allow bypassing CSRF protection of any target URL.	8.8	More Details
CVE-2020-4242	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175419.	8.8	More Details
CVE-2020-4241	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175418.	8.8	More Details
CVE-2020-4238	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 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: 175411.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10882	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the tdpServer service, which listens on UDP port 20002 by default. When parsing the slave_mac parameter, the process does not properly validate 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 the root user. Was ZDI-CAN-9650.	8.8	More Details
CVE-2020-5292	Leantime before versions 2.0.15 and 2.1-beta3 has a SQL Injection vulnerability. The impact is high. Malicious users/attackers can execute arbitrary SQL queries negatively affecting the confidentiality, integrity, and availability of the site. Attackers can exfiltrate data like the users' and administrators' password hashes, modify data, or drop tables. The unescaped parameter is "searchUsers" when sending a POST request to "/tickets/showKanban" with a valid session. In the code, the parameter is named "users" in class.tickets.php. This issue is fixed in versions 2.0.15 and 2.1.0 beta 3.	8.7	More Details
CVE-2020-1764	A hard-coded cryptographic key vulnerability in the default configuration file was found in Kiali, all versions prior to 1.15.1. A remote attacker could abuse this flaw by creating their own JWT signed tokens and bypass Kiali authentication mechanisms, possibly gaining privileges to view and alter the Istio configuration.	8.6	More Details
CVE-2020-3921	UltraLog Express device management software stores user’s information in cleartext. Any user can obtain accounts information through a specific page.	8.6	More Details
CVE-2020-5863	In NGINX Controller versions prior to 3.2.0, an unauthenticated attacker with network access to the Controller API can create unprivileged user accounts. The user which is created is only able to upload a new license to the system but cannot view or modify any other components of the system.	8.6	More Details
CVE-2019-9507	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to command injection because the application incorrectly neutralizes code syntax before executing. Since all commands within the web application are executed as root, this could allow a remote attacker authenticated with an administrator account to execute arbitrary commands as root.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5261	Saml2 Authentication services for ASP.NET (NuGet package Sustainsys.Saml2) greater than 2.0.0, and less than version 2.5.0 has a faulty implementation of Token Replay Detection. Token Replay Detection is an important defence in depth measure for Single Sign On solutions. The 2.5.0 version is patched. Note that version 1.0.1 is not affected. It has a correct Token Replay Implementation and is safe to use. Saml2 Authentication services for ASP.NET (NuGet package Sustainsys.Saml2) greater than 2.0.0, and less than version 2.5.0 have a faulty implementation of Token Replay Detection. Token Replay Detection is an important defense measure for Single Sign On solutions. The 2.5.0 version is patched. Note that version 1.0.1 and prior versions are not affected. These versions have a correct Token Replay Implementation and are safe to use.	8.2	More Details
CVE-2020-10965	Teradici PCoIP Management Console 20.01.0 and 19.11.1 is vulnerable to unauthenticated password resets via login/resetadminpassword of the default admin account. This vulnerability only exists when the default admin account is not disabled. It is fixed in 20.01.1 and 19.11.2.	8.1	More Details
CVE-2020-5860	On BIG-IP 15.0.0-15.1.0.2, 14.1.0-14.1.2.3, 13.1.0-13.1.3.2, 12.1.0-12.1.5.1, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, in a High Availability (HA) network failover in Device Service Cluster (DSC), the failover service does not require a strong form of authentication and HA network failover traffic is not encrypted by Transport Layer Security (TLS).	8.1	More Details
CVE-2020-3920	UltraLog Express device management interface does not properly perform access authentication in some specific pages/functions. Any user can access the privileged page to manage accounts through specific system directory.	8.1	More Details
CVE-2020-10510	Sunnet eHRD, a human training and development management system, contains a vulnerability of Broken Access Control. After login, attackers can use a specific URL, access unauthorized functionality and data.	8.1	More Details
CVE-2019-19127	An authentication bypass vulnerability is present in the standalone SITS:Vision 9.7.0 component of Tribal SITS in its default configuration, related to unencrypted communications sent by the client each time it is launched. This occurs because the Uniface TLS Driver is not enabled by default. This vulnerability allows attackers to gain access to credentials or execute arbitrary SQL queries on the SITS backend as long as they have access to the client executable or can intercept traffic from a user who does.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10940	Local Privilege Escalation can occur in PHOENIX CONTACT PORTICO SERVER through 3.0.7 when installed to run as a service.	7.8	More Details
CVE-2020-10939	Insecure, default path permissions in PHOENIX CONTACT PC WORX SRT through 1.14 allow for local privilege escalation.	7.8	More Details
CVE-2020-9066	Huawei smartphones OxfordP-AN10B with versions earlier than 10.0.1.169(C00E166R4P1) have an improper authentication vulnerability. The Application doesn't perform proper authentication when user performs certain operations. An attacker can trick user into installing a malicious plug-in to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations.	7.8	More Details
CVE-2020-5858	On BIG-IP 15.0.0-15.0.1.2, 14.1.0-14.1.2.2, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, users with non-administrator roles (for example, Guest or Resource Administrator) with tmsh shell access can execute arbitrary commands with elevated privilege via a crafted tmsh command.	7.8	More Details
CVE-2015-8535	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A directory traversal vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2015-8534	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2020-1800	HUAWEI smartphones P30 with versions earlier than 10.0.0.185(C00E85R1P11) have an improper access control vulnerability. The software incorrectly restricts access to a function interface from an unauthorized actor, the attacker tricks the user into installing a crafted application, successful exploit could allow the attacker do certain unauthenticated operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-7333	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type INF and INF_BY_COMPATIBLE_ID command types could allow a user to execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2020-9551	Adobe Bridge versions 10.0 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-9552	Adobe Bridge versions 10.0 have a heap-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	7.8	More Details
CVE-2020-3803	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.	7.8	More Details
CVE-2020-1712	A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	7.8	More Details
CVE-2015-7334	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type COMMAND type could allow a user to execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2020-3766	Adobe Genuine Integrity Service versions Version 6.4 and earlier have an insecure file permissions vulnerability. Successful exploitation could lead to privilege escalation.	7.8	More Details
CVE-2020-10883	This vulnerability allows local attackers to escalate privileges on affected installations of TP-Link Archer A7 Firmware Ver: 190726 AC1750 routers. 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 file system. The issue lies in the lack of proper permissions set on the file system. An attacker can leverage this vulnerability to escalate privileges. Was ZDI-CAN-9651.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10649	DevActSvc.exe in ASUS Device Activation before 1.0.7.0 for Windows 10 notebooks and PCs could lead to unsigned code execution with no additional restrictions when a user puts an application at a particular path with a particular file name.	7.8	More Details
CVE-2020-7944	In Continuous Delivery for Puppet Enterprise (CD4PE) before 3.4.0, changes to resources or classes containing Sensitive parameters can result in the Sensitive parameters ending up in the impact analysis report.	7.7	More Details
CVE-2020-5280	http4s before versions 0.18.26, 0.20.20, and 0.21.2 has a local file inclusion vulnerability. This vulnerability applies to all users of org.http4s.server.staticcontent.FileService, org.http4s.server.staticcontent.ResourceService and org.http4s.server.staticcontent.WebjarService. URI normalization is applied incorrectly. Requests whose path info contain ../ or // can expose resources outside of the configured location. This issue is patched in versions 0.18.26, 0.20.20, and 0.21.2. Note that 0.19.0 is a deprecated release and has never been supported.	7.6	More Details
CVE-2020-5275	In symfony/security-http before versions 4.4.7 and 5.0.7, when a `Firewall` checks access control rule, it iterate overs each rule's attributes and stops as soon as the accessDecisionManager decides to grant access on the attribute, preventing the check of next attributes that should have been take into account in an unanimous strategy. The accessDecisionManager is now called with all attributes at once, allowing the unanimous strategy being applied on each attribute. This issue is patched in versions 4.4.7 and 5.0.7.	7.6	More Details
CVE-2019-17561	The "Apache NetBeans" autoupdate system does not fully validate code signatures. An attacker could modify the downloaded nbm and include additional code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	7.5	More Details
CVE-2020-5859	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file.	7.5	More Details
CVE-2020-2165	Jenkins Artifactory Plugin 3.6.0 and earlier transmits configured passwords in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure.	7.5	More Details
CVE-2020-4214	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to arbitrary delete a directory caused by improper validation of user-supplied input. IBM X-Force ID: 175026.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-11414	An issue was discovered in Progress Telerik UI for Silverlight before 2020.1.330. The RadUploadHandler class in RadUpload for Silverlight expects a web request that provides the file location of the uploading file along with a few other parameters. The uploading file location should be inside the directory where the upload handler class is defined. Before 2020.1.330, a crafted web request could result in uploads to arbitrary locations.	7.5	More Details
CVE-2020-10508	Sunnet eHRD, a human training and development management system, improperly stores system files. Attackers can use a specific URL and capture confidential information.	7.5	More Details
CVE-2020-5857	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service.	7.5	More Details
CVE-2020-9375	TP-Link Archer C50 V3 devices before Build 200318 Rel. 62209 allows remote attackers to cause a denial of service via a crafted HTTP Header containing an unexpected Referer field.	7.5	More Details
CVE-2019-5105	An exploitable memory corruption vulnerability exists in the Name Service Client functionality of 3S-Smart Software Solutions CODESYS GatewayService. A specially crafted packet can cause a large memcpy, resulting in an access violation and termination of the process. An attacker can send a packet to a device running the GatewayService.exe to trigger this vulnerability. All variants of the CODESYS V3 products in all versions prior V3.5.16.10 containing the CmpRouter or CmpRouterEmbedded component are affected, regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PLCnext, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control RTE V3, CODESYS Control RTE V3 (for Beckhoff CX), CODESYS Control Win V3 (also part of the CODESYS Development System setup), CODESYS Control V3 Runtime System Toolkit, CODESYS V3 Embedded Target Visu Toolkit, CODESYS V3 Remote Target Visu Toolkit, CODESYS V3 Safety SIL2, CODESYS Edge Gateway V3, CODESYS Gateway V3, CODESYS HMI V3, CODESYS OPC Server V3, CODESYS PLCHandler SDK, CODESYS V3 Simulation Runtime (part of the CODESYS Development System).	7.5	More Details
CVE-2020-4276	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. X-Force ID: 175984.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-7336	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow the signature check of an update to be bypassed.	7.5	More Details
CVE-2020-5861	On BIG-IP 12.1.0-12.1.5, the TMM process may produce a core file in some cases when Ram Cache incorrectly optimizes stored data resulting in memory errors.	7.5	More Details
CVE-2020-5862	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.2, under certain conditions, TMM may crash or stop processing new traffic with the DPDK/ENA driver on AWS systems while sending traffic. This issue does not affect any other platforms, hardware or virtual, or any other cloud provider since the affected driver is specific to AWS.	7.5	More Details
CVE-2020-3800	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have a memory address leak vulnerability. Successful exploitation could lead to information disclosure .	7.5	More Details
CVE-2020-3761	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a remote file read vulnerability. Successful exploitation could lead to arbitrary file read from the coldfusion install directory.	7.5	More Details
CVE-2020-8509	Zoho ManageEngine Desktop Central before 10.0.483 allows unauthenticated users to access PDFGenerationServlet, leading to sensitive information disclosure.	7.5	More Details
CVE-2020-5724	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	7.5	More Details
CVE-2020-3777	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	7.5	More Details
CVE-2020-6809	When a Web Extension had the all-urls permission and made a fetch request with a mode set to 'same-origin', it was possible for the Web Extension to read local files. This vulnerability affects Firefox < 74.	7.5	More Details
CVE-2020-5129	A vulnerability in the SonicWall SMA1000 HTTP Extraweb server allows an unauthenticated remote attacker to cause HTTP server crash which leads to Denial of Service. This vulnerability affected SMA1000 Version 12.1.0-06411 and earlier.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5527	When MELSOFT transmission port (UDP/IP) of Mitsubishi Electric MELSEC iQ-R series (all versions), MELSEC iQ-F series (all versions), MELSEC Q series (all versions), MELSEC L series (all versions), and MELSEC F series (all versions) receives massive amount of data via unspecified vectors, resource consumption occurs and the port does not process the data properly. As a result, it may fall into a denial-of-service (DoS) condition. The vendor states this vulnerability only affects Ethernet communication functions.	7.5	More Details
CVE-2020-3769	Adobe Experience Manager versions 6.5 and earlier have a server-side request forgery (ssrf) vulnerability. Successful exploitation could lead to sensitive information disclosure.	7.5	More Details
CVE-2020-5726	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	7.5	More Details
CVE-2020-6095	An exploitable denial of service vulnerability exists in the GstRTSPAuth functionality of GStreamer/gst-rtsp-server 1.14.5. A specially crafted RTSP setup request can cause a null pointer deference resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2020-10954	GitLab through 12.9 is affected by a potential DoS in repository archive download.	7.5	More Details
CVE-2020-10953	In GitLab EE 11.7 through 12.9, the NPM feature is vulnerable to a path traversal issue.	7.5	More Details
CVE-2020-3806	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	7.5	More Details
CVE-2020-3804	Adobe Acrobat and Reader versions 2020.006.20034 and earlier, 2017.011.30158 and earlier, 2017.011.30158 and earlier, 2015.006.30510 and earlier, and 2015.006.30510 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	7.5	More Details
CVE-2020-7260	DLL Side Loading vulnerability in the installer for McAfee Application and Change Control (MACC) prior to 8.3 allows local users to execute arbitrary code via execution from a compromised folder.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1773	An attacker with the ability to generate session IDs or password reset tokens, either by being able to authenticate or by exploiting OSA-2020-09, may be able to predict other users session IDs, password reset tokens and automatically generated passwords. This issue affects ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS; 7.0.15 and prior versions.	7.3	More Details
CVE-2020-5282	In Nick Chan Bot before version 1.0.0-beta there is a vulnerability in the `npm` command which is part of this software package. This allows arbitrary shell execution,which can compromise the bot This is patched in version 1.0.0-beta	7.2	More Details
CVE-2019-7245	An issue was discovered in GPU-Z.sys in TechPowerUp GPU-Z before 2.23.0. The vulnerable driver exposes a wrmsr instruction via an IOCTL and does not properly filter the Model Specific Register (MSR). Allowing arbitrary MSR writes can lead to Ring-0 code execution and escalation of privileges.	7.2	More Details
CVE-2019-7244	An issue was discovered in kerneld.sys in AIDA64 before 5.99. The vulnerable driver exposes a wrmsr instruction via IOCTL 0x80112084 and does not properly filter the Model Specific Register (MSR). Allowing arbitrary MSR writes can lead to Ring-0 code execution and escalation of privileges.	7.2	More Details
CVE-2019-7240	An issue was discovered in WinRing0x64.sys in Moo0 System Monitor 1.83. The vulnerable driver exposes a wrmsr instruction via IOCTL 0x9C402088 and does not properly filter the Model Specific Register (MSR). Allowing arbitrary MSR writes can lead to Ring-0 code execution and escalation of privileges.	7.2	More Details
CVE-2020-10963	FrozenNode Laravel-Administrator through 5.0.12 allows unrestricted file upload (and consequently Remote Code Execution) via admin/tips_image/image/file_upload image upload with PHP content within a GIF image that has the .php extension. NOTE: this product is discontinued.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5291	Bubblewrap (bwrap) before version 0.4.1, if installed in setuid mode and the kernel supports unprivileged user namespaces, then the `bwrap --userns2` option can be used to make the setuid process keep running as root while being traceable. This can in turn be used to gain root permissions. Note that this only affects the combination of bubblewrap in setuid mode (which is typically used when unprivileged user namespaces are not supported) and the support of unprivileged user namespaces. Known to be affected are: * Debian testing/unstable, if unprivileged user namespaces enabled (not default) * Debian buster-backports, if unprivileged user namespaces enabled (not default) * Arch if using `linux-hardened`, if unprivileged user namespaces enabled (not default) * Centos 7 flatpak COPR, if unprivileged user namespaces enabled (not default) This has been fixed in the 0.4.1 release, and all affected users should update.	7.2	More Details
CVE-2019-7630	An issue was discovered in gdrv.sys in Gigabyte APP Center before 19.0227.1. The vulnerable driver exposes a wrmsr instruction via IOCTL 0xC3502580 and does not properly filter the target Model Specific Register (MSR). Allowing arbitrary MSR writes can lead to Ring-0 code execution and escalation of privileges.	7.2	More Details
CVE-2015-7335	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A race condition was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow a user to execute arbitrary code with elevated privileges.	7.0	More Details
CVE-2020-5344	Dell EMC iDRAC7, iDRAC8 and iDRAC9 versions prior to 2.65.65.65, 2.70.70.70, 4.00.00.00 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input data.	7.0	More Details
CVE-2020-5289	In Elide before 4.5.14, it is possible for an adversary to "guess and check" the value of a model field they do not have access to assuming they can read at least one other field in the model. The adversary can construct filter expressions for an inaccessible field to filter a collection. The presence or absence of models in the returned collection can be used to reconstruct the value of the inaccessible field. Resolved in Elide 4.5.14 and greater.	6.8	More Details
CVE-2020-10955	GitLab EE/CE 11.1 through 12.9 is vulnerable to parameter tampering on an upload feature that allows an unauthorized user to read content available under specific folders.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-10952	GitLab EE/CE 8.11 through 12.9.1 allows blocked users to pull/push docker images.	6.5	More Details
CVE-2020-7599	All versions of com.gradle.plugin-publish before 0.11.0 are vulnerable to Insertion of Sensitive Information into Log File. When a plugin author publishes a Gradle plugin while running Gradle with the --info log level flag, the Gradle Logger logs an AWS pre-signed URL. If this build log is publicly visible (as it is in many popular public CI systems like TravisCI) this AWS pre-signed URL would allow a malicious actor to replace a recently uploaded plugin with their own.	6.5	More Details
CVE-2020-6808	When a JavaScript URL (javascript:) is evaluated and the result is a string, this string is parsed to create an HTML document, which is then presented. Previously, this document's URL (as reported by the document.location property, for example) was the originating javascript: URL which could lead to spoofing attacks; it is now correctly the URL of the originating document. This vulnerability affects Firefox < 74.	6.5	More Details
CVE-2020-4236	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow an authenticated user to cause a denial of service due to improper content parsing in the project management module. IBM X-Force ID: 175409.	6.5	More Details
CVE-2020-2164	Jenkins Artifactory Plugin 3.5.0 and earlier stores its Artifactory server password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	6.5	More Details
CVE-2020-10966	In the Password Reset Module in VESTA Control Panel through 0.9.8-25 and Hestia Control Panel before 1.1.1, Host header manipulation leads to account takeover because the victim receives a reset URL containing an attacker-controlled server name.	6.5	More Details
CVE-2020-8910	A URL parsing issue in goog.uri of the Google Closure Library versions up to and including v20200224 allows an attacker to send malicious URLs to be parsed by the library and return the wrong authority. Mitigation: update your library to version v20200315.	6.5	More Details
CVE-2020-4240	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request to overwrite or create arbitrary files on the system. IBM X-Force ID: 175417.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-1772	It's possible to craft Lost Password requests with wildcards in the Token value, which allows attacker to retrieve valid Token(s), generated by users which already requested new passwords. This issue affects: ((OTRS)) Community Edition 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	6.5	More Details
CVE-2020-6999	In Moxa EDS-G516E Series firmware, Version 5.2 or lower, some of the parameters in the setting pages do not ensure text is the correct size for its buffer.	6.5	More Details
CVE-2020-10791	app/Plugin/GrafanaModule/Controller/GrafanaConfigurationController.php in openITCOCKPIT before 3.7.3 allows remote authenticated users to trigger outbound TCP requests (aka SSRF) via the Test Connection feature (aka testGrafanaConnection) of the Grafana Module.	6.5	More Details
CVE-2019-9509	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to reflected XSS in an HTTP POST parameter. The web application does not neutralize user-controllable input before displaying to users in a web page, which could allow a remote attacker authenticated with a user account to execute arbitrary code.	6.3	More Details
CVE-2019-9508	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to stored XSS. A remote attacker authenticated with an administrator account could store a maliciously named file within the web application that would execute each time a user browsed to the page.	6.3	More Details
CVE-2020-5281	In Perun before version 3.9.1, VO or group manager can modify configuration of the LDAP extSource to retrieve all from Perun LDAP. Issue is fixed in version 3.9.1 by sanitisation of the input.	6.2	More Details
CVE-2020-11441	phpMyAdmin 5.0.2 allows CRLF injection, as demonstrated by %0D%0Astring%0D%0A inputs to login form fields causing CRLF sequences to be reflected on an error page. NOTE: the vendor states "I don't see anything specifically exploitable.	6.1	More Details
CVE-2020-5559	Cross-site scripting vulnerability in WL-Enq 1.11 and 1.12 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	6.1	More Details
CVE-2020-11106	An issue was discovered in Responsive Filemanager through 9.14.0. In the dialog.php page, the session variable $_SESSION['RF']["view_type"] wasn't sanitized if it was already set. This made stored XSS possible if one opens ajax_calls.php and uses the "view" action and places a payload in the type parameter, and then returns to the dialog.php page. This occurs because ajax_calls.php was also able to set the $_SESSION['RF']["view_type"] variable, but there it wasn't sanitized.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5557	Cross-site scripting vulnerability in CuteNews 2.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	6.1	More Details
CVE-2020-5552	Cross-site scripting vulnerability in mailform version 1.04 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	6.1	More Details
CVE-2020-10509	Sunnet eHRD, a human training and development management system, contains vulnerability of Cross-Site Scripting (XSS), attackers can inject arbitrary command into the system and launch XSS attack.	6.1	More Details
CVE-2020-2169	A form validation endpoint in Jenkins Queue cleanup Plugin 1.3 and earlier does not properly escape a query parameter displayed in an error message, resulting in a reflected XSS vulnerability.	6.1	More Details
CVE-2020-5725	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords.	5.9	More Details
CVE-2020-3808	Creative Cloud Desktop Application versions 5.0 and earlier have a time-of-check to time-of-use (toctou) race condition vulnerability. Successful exploitation could lead to arbitrary file deletion.	5.9	More Details
CVE-2020-10560	An issue was discovered in Open Source Social Network (OSSN) through 5.3. A user-controlled file path with a weak cryptographic rand() can be used to read any file with the permissions of the webserver. This can lead to further compromise. The attacker must conduct a brute-force attack against the SiteKey to insert into a crafted URL for components/OssnComments/ossn_com.php and/or libraries/ossn.lib.upgrade.php.	5.9	More Details
CVE-2019-14905	A vulnerability was found in Ansible Engine versions 2.9.x before 2.9.3, 2.8.x before 2.8.8, 2.7.x before 2.7.16 and earlier, where in Ansible's nxos_file_copy module can be used to copy files to a flash or bootflash on NXOS devices. Malicious code could craft the filename parameter to perform OS command injections. This could result in a loss of confidentiality of the system among other issues.	5.6	More Details
CVE-2020-9065	Huawei smart phone Taurus-AL00B with versions earlier than 10.0.0.203(C00E201R7P2) have a use-after-free (UAF) vulnerability. An authenticated, local attacker may perform specific operations to exploit this vulnerability. Successful exploitation may tamper with the information to affect the availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-20633	GNU patch through 2.7.6 contains a free(p_line[p_end]) Double Free vulnerability in the function another_hunk in pch.c that can cause a denial of service via a crafted patch file. NOTE: this issue exists because of an incomplete fix for CVE-2018-6952.	5.5	More Details
CVE-2020-2170	Jenkins RapidDeploy Plugin 4.2 and earlier does not escape package names in the table of packages obtained from a remote server, resulting in a stored XSS vulnerability.	5.4	More Details
CVE-2020-10790	openITCOCKPIT before 3.7.3 has unnecessary files (such as Lodash files) under the web root, which leads to XSS.	5.4	More Details
CVE-2019-13495	In firmware version 4.50 of Zyxel XGS2210-52HP, multiple stored cross-site scripting (XSS) issues allows remote authenticated users to inject arbitrary web script via an rpSys.html Name or Location field.	5.4	More Details
CVE-2020-2163	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier improperly processes HTML content of list view column headers, resulting in a stored XSS vulnerability exploitable by users able to control column headers.	5.4	More Details
CVE-2020-2162	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not set Content-Security-Policy headers for files uploaded as file parameters to a build, resulting in a stored XSS vulnerability.	5.4	More Details
CVE-2020-2161	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not properly escape node labels that are shown in the form validation for label expressions on job configuration pages, resulting in a stored XSS vulnerability exploitable by users able to define node labels.	5.4	More Details
CVE-2020-4235	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 175408.	5.4	More Details
CVE-2020-7918	An insecure direct object reference in webmail in totemo totemomail 7.0.0 allows an authenticated remote user to read and modify mail folder names of other users via enumeration.	5.4	More Details
CVE-2020-9520	A stored XSS vulnerability was discovered in Micro Focus Vibe, affecting all Vibe version prior to 4.0.7. The vulnerability could allows a remote attacker to craft and store malicious content into Vibe such that when the content is viewed by another user of the system, attacker controlled JavaScript will execute in the security context of the target user’s browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-9467	Piwigo 2.10.1 has stored XSS via the file parameter in a /ws.php request because of the pwg.images.setInfo function.	5.4	More Details
CVE-2020-8923	An improper HTML sanitization in Dart versions up to and including 2.7.1 and dev versions 2.8.0-dev.16.0, allows an attacker leveraging DOM Clobbering techniques to skip the sanitization and inject custom html/javascript (XSS). Mitigation: update your Dart SDK to 2.7.2, and 2.8.0-dev.17.0 for the dev version. If you cannot update, we recommend you review the way you use the affected APIs, and pay special attention to cases where user-provided data is used to populate DOM nodes. Consider using Element.innerText or Node.text to populate DOM elements.	5.4	More Details
CVE-2020-6812	The first time AirPods are connected to an iPhone, they become named after the user's name by default (e.g. Jane Doe's AirPods.) Websites with camera or microphone permission are able to enumerate device names, disclosing the user's name. To resolve this issue, Firefox added a special case that renames devices containing the substring 'AirPods' to simply 'AirPods'. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.	5.3	More Details
CVE-2020-11104	An issue was discovered in USC iLab cereal through 1.3.0. Serialization of an (initialized) C/C++ long double variable into a BinaryArchive or PortableBinaryArchive leaks several bytes of stack or heap memory, from which sensitive information (such as memory layout or private keys) can be gleaned if the archive is distributed outside of a trusted context.	5.3	More Details
CVE-2020-8552	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.	5.3	More Details
CVE-2020-4239	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 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: 175412.	5.3	More Details
CVE-2020-6813	When protecting CSS blocks with the nonce feature of Content Security Policy, the @import statement in the CSS block could allow an attacker to inject arbitrary styles, bypassing the intent of the Content Security Policy. This vulnerability affects Firefox < 74.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5340	RSA Authentication Manager versions prior to 8.4 P10 contain a stored cross-site scripting vulnerability in the Security Console. A malicious RSA Authentication Manager Security Console administrator with advanced privileges could exploit this vulnerability to store arbitrary HTML or JavaScript code through the Security Console web interface. When other Security Console administrators attempt to change the default security domain mapping, the injected scripts could potentially be executed in their browser.	4.8	More Details
CVE-2020-5339	RSA Authentication Manager versions prior to 8.4 P10 contain a stored cross-site scripting vulnerability in the Security Console. A malicious RSA Authentication Manager Security Console administrator with advanced privileges could exploit this vulnerability to store arbitrary HTML or JavaScript code through the Security Console web interface. When other Security Console administrators open the affected report page, the injected scripts could potentially be executed in their browser.	4.8	More Details
CVE-2019-19913	In Intland codeBeamer ALM 9.5 and earlier, there is stored XSS via the Trackers Title parameter.	4.8	More Details
CVE-2019-19912	In Intland codeBeamer ALM 9.5 and earlier, a cross-site scripting (XSS) vulnerability in the Upload Flash File feature allows authenticated remote attackers to inject arbitrary scripts via an active script embedded in an SWF file.	4.8	More Details
CVE-2019-15795	python-apt only checks the MD5 sums of downloaded files in `Version.fetch_binary()` and `Version.fetch_source()` of apt/package.py in version 1.9.0ubuntu1 and earlier. This allows a man-in-the-middle attack which could potentially be used to install altered packages and has been fixed in versions 1.9.0ubuntu1.2, 1.6.5ubuntu0.1, 1.1.0~beta1ubuntu0.16.04.7, 0.9.3.5ubuntu3+esm2, and 0.8.3ubuntu7.5.	4.7	More Details
CVE-2019-15796	Python-apt doesn't check if hashes are signed in `Version.fetch_binary()` and `Version.fetch_source()` of apt/package.py or in `_fetch_archives()` of apt/cache.py in version 1.9.3ubuntu2 and earlier. This allows downloads from unsigned repositories which shouldn't be allowed and has been fixed in verisions 1.9.5, 1.9.0ubuntu1.2, 1.6.5ubuntu0.1, 1.1.0~beta1ubuntu0.16.04.7, 0.9.3.5ubuntu3+esm2, and 0.8.3ubuntu7.5.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5274	In Symfony before versions 5.0.5 and 4.4.5, some properties of the Exception were not properly escaped when the `ErrorHandler` rendered it stacktrace. In addition, the stacktrace were displayed even in a non-debug configuration. The ErrorHandler now escape alls properties of the exception, and the stacktrace is only display in debug configuration. This issue is patched in symfony/http-foundation versions 4.4.5 and 5.0.5	4.6	More Details
CVE-2020-1771	Attacker is able craft an article with a link to the customer address book with malicious content (JavaScript). When agent opens the link, JavaScript code is executed due to the missing parameter encoding. This issue affects: ((OTRS)) Community Edition: 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	4.6	More Details
CVE-2020-5284	Next.js versions before 9.3.2 have a directory traversal vulnerability. Attackers could craft special requests to access files in the dist directory (.next). This does not affect files outside of the dist directory (.next). In general, the dist directory only holds build assets unless your application intentionally stores other assets under this directory. This issue is fixed in version 9.3.2.	4.4	More Details
CVE-2020-3791	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	4.3	More Details
CVE-2020-6810	After a website had entered fullscreen mode, it could have used a previously opened popup to obscure the notification that indicates the browser is in fullscreen mode. Combined with spoofing the browser chrome, this could have led to confusing the user about the current origin of the page and credential theft or other attacks. This vulnerability affects Firefox < 74.	4.3	More Details
CVE-2020-3771	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	4.3	More Details
CVE-2020-9468	The Community plugin 2.9.e-beta for Piwigo allows users to set image information on images in albums for which they do not have permission, by manipulating the image_id parameter.	4.3	More Details
CVE-2019-18626	Harris Ormed Self Service before 2019.1.4 allows an authenticated user to view W-2 forms belonging to other users via an arbitrary empNo value to the ORMEDMIS/Data/PY/T4W2Service.svc/RetrieveW2EntriesForEmployee URI, thus exposing sensitive information including employee tax information, social security numbers, home addresses, and more.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-8551	The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.	4.3	More Details
CVE-2020-3781	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	4.3	More Details
CVE-2020-3778	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	4.3	More Details
CVE-2020-3782	Adobe Photoshop CC 2019 versions 20.0.8 and earlier, and Photoshop 2020 versions 21.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	4.3	More Details
CVE-2019-2391	Incorrect parsing of certain JSON input may result in js-bson not correctly serializing BSON. This may cause unexpected application behaviour including data disclosure. This issue affects: MongoDB Inc. js-bson library version 1.1.3 and prior to.	4.2	More Details
CVE-2020-5277	PrestaShop module ps_facetedsearch versions before 3.5.0 has a reflected XSS with `url_name` parameter. The problem is fixed in 3.5.0	4.1	More Details
CVE-2020-9055	Versiant LYNX Customer Service Portal (CSP), version 3.5.2, is vulnerable to stored cross-site scripting, which could allow a local, authenticated attacker to insert malicious JavaScript that is stored and displayed to the end user. This could lead to website redirects, session cookie hijacking, or information disclosure.	3.9	More Details
CVE-2019-20634	An issue was discovered in Proofpoint Email Protection through 2019-09-08. By collecting scores from Proofpoint email headers, it is possible to build a copy-cat Machine Learning Classification model and extract insights from this model. The insights gathered allow an attacker to craft emails that receive preferable scores, with a goal of delivering malicious emails.	3.7	More Details
CVE-2020-1769	In the login screens (in agent and customer interface), Username and Password fields use autocomplete, which might be considered as security issue. This issue affects: ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5255	In Symfony before versions 4.4.7 and 5.0.7, when a `Response` does not contain a `Content-Type` header, affected versions of Symfony can fallback to the format defined in the `Accept` header of the request, leading to a possible mismatch between the response's content and `Content-Type` header. When the response is cached, this can prevent the use of the website by other users. This has been patched in versions 4.4.7 and 5.0.7.	2.6	More Details
CVE-2020-1770	Support bundle generated files could contain sensitive information that might be unwanted to be disclosed. This issue affects: ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2.4	More Details
CVE-2019-10180	A vulnerability was found in all pki-core 10.x.x version, where the Token Processing Service (TPS) did not properly sanitize several parameters stored for the tokens, possibly resulting in a Stored Cross Site Scripting (XSS) vulnerability. An attacker able to modify the parameters of any token could use this flaw to trick an authenticated user into executing arbitrary JavaScript code.	2.4	More Details