UgCERT
UGANDA COMPUTER EMERGENCY RESPONSE TEAM

Vulnerability Summary for the Week of January 18, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave_glass	There is a vulnerability caused by unsafe Java deserialization that allows for arbitrary command execution in a containerized environment within Airwave Glass before 1.3.3. Successful exploitation can lead to complete compromise of the underlying host operating system.	2021-01-15	10	CVE-2020-24639 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- airwave_glass	Multiple authenticated remote command executions are possible in Airwave Glass before 1.3.3 via the glassadmin cli. These allow for a user with glassadmin privileges to execute arbitrary code as root on the underlying host operating system.	2021-01-15	9	CVE-2020-24638 MISC
arubanetworks -- airwave_glass	There is a vulnerability caused by insufficient input validation that allows for arbitrary command execution in a containerized environment within Airwave Glass before 1.3.3. Successful exploitation can lead to complete compromise of the underlying host operating system.	2021-01-15	10	CVE-2020-24640 MISC
fasterxml -- jackson-databind	A flaw was found in jackson-databind before 2.9.10.7. FasterXML mishandles the interaction between serialization gadgets and typing. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-01-19	8.3	CVE-2021-20190 MISC MISC
hgiga -- oaklouds_openid	HGiga EIP product contains SQL Injection vulnerability. Attackers can inject SQL commands into specific URL parameter (document management page) to obtain database schema and data.	2021-01-19	7.5	CVE-2021-22851 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hgiga -- oaklouds_portal	HGiga EIP product lacks ineffective access control in certain pages that allow attackers to access database or perform privileged functions.	2021-01-19	7.5	CVE-2021-22850 CONFIRM CONFIRM
ibm -- security_guardium	IBM Security Guardium 10.6 and 11.2 could allow a local attacker to execute arbitrary commands on the system as an unprivileged user, caused by command injection vulnerability. IBM X-Force ID: 186700.	2021-01-20	7.2	CVE-2020-4688 XF CONFIRM
jointjs -- jointjs	The package jointjs before 3.3.0 are vulnerable to Prototype Pollution via util.setByPath (https://resources.jointjs.com/docs/jointjs/v3.2/joint.htmlutil.setByPath). The path used the access the object's key and set the value is not properly sanitized, leading to a Prototype Pollution.	2021-01-19	7.5	CVE-2020-28480 MISC MISC MISC MISC MISC
juniper -- contrail_networking	An Information Exposure vulnerability in Juniper Networks Contrail Networking allows a locally authenticated attacker able to read files to retrieve administrator credentials stored in plaintext thereby elevating their privileges over the system. This issue affects: Juniper Networks Contrail Networking versions prior to 1911.31.	2021-01-15	7.2	CVE-2021-0212 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos	A command injection vulnerability in install package validation subsystem of Juniper Networks Junos OS that may allow a locally authenticated attacker with privileges to execute commands with root privilege. To validate a package in Junos before installation, an administrator executes the command 'request system software add validate-on-host' via the CLI. An attacker with access to this CLI command may be able to exploit this vulnerability. This issue affects Juniper Networks Junos OS: all versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R2-S8, 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2.	2021-01-15	7.2	CVE-2021-0219 CONFIRM
juniper -- junos	A command injection vulnerability in the license-check daemon of Juniper Networks Junos OS that may allow a locally authenticated attacker with low privileges to execute commands with root privilege. license-check is a daemon used to manage licenses in Junos OS. To update licenses, a user executes the command 'request	2021-01-15	7.2	CVE-2021-0218 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system license update' via the CLI. An attacker with access to this CLI command may be able to exploit the vulnerability. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.			
juniper -- junos	A sensitive information disclosure vulnerability in delta-export configuration utility (dexp) of Juniper Networks Junos OS may allow a locally authenticated shell user the ability to create and read database files generated by the dexp utility, including password hashes of local users. Since dexp is shipped with setuid permissions enabled and is owned by the root user, this vulnerability may allow a local privileged user the ability to run dexp with root privileges and access sensitive information in the dexp database. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S8; 15.1X49 versions prior to 15.1X49-D230; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to	2021-01-15	7.2	CVE-2021-0204 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D34; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3-S1; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.			
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, AttachmentUploadServlet also saves user controlled data (`request.getInputStream()`) to a user specified location (`request.getHeader("File-Name")`). This issue may lead to arbitrary file upload which can be used to upload a WebShell to OneDev server. This issue is addressed in 4.0.3 by only allowing uploaded file to be in attachments folder. The webshell issue is not possible as OneDev never executes files in attachments folder.	2021-01-15	7.5	CVE-2021-21245 MISC CONFIRM
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, There is a vulnerability that enabled pre-auth server side template injection via Bean validation message tampering. Full details in the	2021-01-15	7.5	CVE-2021-21244 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reference GHSA. This issue was fixed in 4.0.3 by disabling validation interpolation completely.			
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, a Kubernetes REST endpoint exposes two methods that deserialize untrusted data from the request body. These endpoints do not enforce any authentication or authorization checks. This issue may lead to pre-auth RCE. This issue was fixed in 4.0.3 by not using deserialization at KubernetesResource side.	2021-01-15	7.5	CVE-2021-21243 MISC CONFIRM
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is a critical vulnerability which can lead to pre-auth remote code execution. AttachmentUploadServlet deserializes untrusted data from the `Attachment-Support` header. This Servlet does not enforce any authentication or authorization checks. This issue may lead to pre-auth remote code execution. This issue was fixed in 4.0.3 by removing AttachmentUploadServlet and not using deserialization	2021-01-15	7.5	CVE-2021-21242 MISC CONFIRM
oracle -- coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily	2021-01-20	7.5	CVE-2020-14756 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
oracle -- enterprise_repository	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2021-01-20	7.5	CVE-2021-1994 MISC
oracle -- mysql	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this	2021-01-20	7.1	CVE-2021-2011 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	2021-01-20	7	CVE-2021-2048 MISC
oracle -- scripting	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Miscellaneous). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful	2021-01-20	7.5	CVE-2021-2029 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacks of this vulnerability can result in takeover of Oracle Scripting. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
prestashop -- prestashop	The store system in PrestaShop 1.7.7.0 allows time-based boolean SQL injection via the module=productcomments controller=CommentGrade id_products[] parameter.	2021-01-20	7.5	CVE-2021-3110 MISC MISC
the-guild -- graphql-tools	This affects the package @graphql-tools/git-loader before 6.2.6. The use of exec and execSync in packages/loaders/git/src/load-git.ts allows arbitrary command injection.	2021-01-20	7.5	CVE-2021-23326 MISC MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
anchorcms -- anchor_cms	A CSRF vulnerability exists in Anchor CMS 0.12.7 anchor/views/users/edit.php that can change the Delete admin users.	2021-01-19	6.8	CVE-2020-23342 MISC MISC MISC
apache -- guacamole	Apache Guacamole 1.2.0 and earlier do not consistently restrict access to connection history based on user visibility. If multiple users share access to the same connection, those users may be able to see which other users have accessed that connection, as well as the IP addresses from which that connection was accessed, even if those users do not otherwise have permission to see other users.	2021-01-19	4	CVE-2020-11997 MISC
arubanetworks -- airwave_glass	In Aruba AirWave Glass before 1.3.3, there is a Server-Side Request Forgery vulnerability through an unauthenticated endpoint that if successfully exploited can result in disclosure of sensitive information. This can be used to perform an authentication bypass and ultimately gain administrative access on the web administrative interface.	2021-01-15	5	CVE-2020-24641 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- confluence	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the avatar upload feature. The affected versions are before version 7.2.0.	2021-01-19	4	CVE-2020-29450 MISC
docker -- docker	Docker Desktop Community before 2.5.0.0 on macOS mishandles certificate checking, leading to local privilege escalation.	2021-01-15	4.6	CVE-2021-3162 MISC MISC
erlang -- otp	An issue was discovered in Erlang/OTP before 23.2.2. The ssl application 10.2 accepts and trusts an invalid X.509 certificate chain to a trusted root Certification Authority.	2021-01-15	5	CVE-2020-35733 CONFIRM MISC MISC MISC
fhem -- fhem	Local file inclusion in FHEM 6.0 allows in fhem/FileLog_logWrapper file parameter can allow an attacker to include a file, which can lead to sensitive information disclosure.	2021-01-20	5	CVE-2020-19360 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flatcore -- flatcore	An issue was discovered in flatCore before 2.0.0 build 139. A time-based blind SQL injection was identified in the selected_folder HTTP request body parameter for the acp interface. The affected parameter (which retrieves the file contents of the specified folder) was found to be accepting malicious user input without proper sanitization, thus leading to SQL injection. Database related information can be successfully retrieved.	2021-01-15	4	CVE-2021-23837 MISC MISC MISC
flatcore -- flatcore	An issue was discovered in flatCore before 2.0.0 build 139. A local file disclosure vulnerability was identified in the docs_file HTTP request body parameter for the acp interface. This can be exploited with admin access rights. The affected parameter (which retrieves the contents of the specified file) was found to be accepting malicious user input without proper sanitization, thus leading to retrieval of backend server sensitive files, e.g., /etc/passwd, SQLite database files, PHP source code, etc.	2021-01-15	4	CVE-2021-23835 MISC MISC MISC
gitlab -- gitlab	A regular expression denial of service issue has been discovered in NuGet API affecting all versions of GitLab starting from version 12.8.	2021-01-15	4	CVE-2021-22168 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions starting from 12.4. The regex used for package names is written in a way that makes execution time have quadratic growth based on the length of the malicious input string.	2021-01-15	4	CVE-2020-26414 CONFIRM MISC
gitlab -- gitlab	Insufficient validation of authentication parameters in GitLab Pages for GitLab 11.5+ allows an attacker to steal a victim's API token if they click on a maliciously crafted link	2021-01-15	4.3	CVE-2021-22171 CONFIRM MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions starting from 12.1. Incorrect headers in specific project page allows attacker to have a temporary read access to the private repository	2021-01-15	5	CVE-2021-22167 CONFIRM MISC MISC
gitlab -- gitlab	An attacker could cause a Prometheus denial of service in GitLab 13.7+ by sending an HTTP request with a malformed method	2021-01-15	5	CVE-2021-22166 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
greensock -- greensock_animation_platform	This affects the package gsap before 3.6.0.	2021-01-19	5	CVE-2020-28478 MISC MISC
hgiga -- oaklouds_openid	HGiga EIP product contains SQL Injection vulnerability. Attackers can inject SQL commands into specific URL parameter (online registration) to obtain database schema and data.	2021-01-19	6.5	CVE-2021-22852 CONFIRM CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could allow an attacker to obtain sensitive information due to an overly permissive CORS policy. IBM X-Force ID: 190836.	2021-01-19	5	CVE-2020-4873 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the lack of server hostname verification for SSL/TLS communication. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 190851.	2021-01-19	5	CVE-2020-4881 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_guardium	IBM Security Guardium 10.6 and 11.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 191398.	2021-01-20	6.5	CVE-2020-4921 XF CONFIRM
ibm -- spectrum_lsf	IBM Spectrum LSF 10.1 and IBM Spectrum LSF Suite 10.2 could allow a user on the local network who has privileges to submit LSF jobs to execute arbitrary commands. IBM X-Force ID: 192586.	2021-01-20	4.6	CVE-2020-4983 XF CONFIRM
immer_project -- immer	This affects all versions of package immer.	2021-01-19	5	CVE-2020-28477 MISC MISC MISC
jointjs -- jointjs	The package jointjs before 3.3.0 are vulnerable to Denial of Service (DoS) via the unsetByPath function.	2021-01-19	5	CVE-2020-28479 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos	An improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved Routing Protocol Daemon (RPD) service allows an attacker to send a valid BGP FlowSpec message thereby causing an unexpected change in the route advertisements within the BGP FlowSpec domain leading to disruptions in network traffic causing a Denial of Service (DoS) condition. Continued receipt of these update messages will cause a sustained Denial of Service condition. This issue affects Juniper Networks: Junos OS: All versions prior to 17.3R3-S10 with the exceptions of 15.1X49-D240 on SRX Series and 15.1R7-S8 on EX Series; 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R1-S3, 19.4R2-S3, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S3 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2. Junos OS Evolved: All versions prior to 20.3R1-S1-EVO, 20.3R2-EVO.	2021-01-15	6.4	CVE-2021-0211 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos	An Information Exposure vulnerability in J-Web of Juniper Networks Junos OS allows an unauthenticated attacker to elevate their privileges over the target system through opportunistic use of an authenticated users session. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S17; 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R2-S4, 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3, 19.2R3-S1; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2.	2021-01-15	5	CVE-2021-0210 CONFIRM
juniper -- junos	An improper interpretation conflict of certain data between certain software components within the Juniper Networks Junos OS devices does not allow certain traffic to pass through the device upon receipt from an ingress interface filtering certain specific types of traffic which is then being redirected to an egress interface on a different VLAN. This causes a Denial of Service (DoS) to those clients sending these particular types of traffic. Such traffic being sent by a client may appear genuine, but is non-standard in nature and should be	2021-01-15	5	CVE-2021-0207 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	considered as potentially malicious, and can be targeted to the device, or destined through it for the issue to occur. This issues affects IPv4 and IPv6 traffic. An indicator of compromise may be found by checking log files. You may find that traffic on the input interface has 100% of traffic flowing into the device, yet the egress interface shows 0 pps leaving the device. For example: [show interfaces "interface" statistics detail] Output between two interfaces would reveal something similar to: Ingress, first interface: -------------------- Interface Link Input packets (pps) Output packets (pps) et-0/0/0 Up 9999999999 (9999) 1 (0) -------------------- Egress, second interface: -------------------- Interface Link Input packets (pps) Output packets (pps) et-0/0/1 Up 0 (0) 9999999999 (0) -------------------- Dropped packets will not show up in DDoS monitoring/protection counters as issue is not caused by anti-DDoS protection mechanisms. This issue affects: Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S7 on NFX250, QFX5K Series, EX4600; 17.4 versions prior to 17.4R2-S11, 17.4R3-S3 on NFX250, QFX5K Series, EX4600; 18.1 versions prior to 18.1R3-S9 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4600; 18.2 versions prior to 18.2R3-S3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600; 18.3 versions prior to 18.3R3-S1 on NFX250, QFX5K			

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.2 versions prior to 19.2R1-S5, 19.2R2 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.3 versions prior to 19.3R2-S3, 19.3R3 on NFX250, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series; 19.4 versions prior to 19.4R1-S2, 19.4R2 on NFX250, NFX350, QFX5K Series, EX2300 Series, EX3400 Series, EX4300 Multigigabit, EX4600 Series. This issue does not affect Junos OS releases prior to 17.2R2.			
juniper -- junos	A NULL Pointer Dereference vulnerability in Juniper Networks Junos OS allows an attacker to send a specific packet causing the packet forwarding engine (PFE) to crash and restart, resulting in a Denial of Service (DoS). By continuously sending these specific packets, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue only affects Juniper Networks NFX Series, SRX Series platforms when SSL Proxy is configured. This issue	2021-01-15	5	CVE-2021-0206 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affects Juniper Networks Junos OS on NFX Series and SRX Series: 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S1; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S2, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS versions on NFX Series and SRX Series prior to 18.3R1.			
juniper -- junos	On Juniper Networks MX Series and EX9200 Series platforms with Trio-based MPC (Modular Port Concentrator) where Integrated Routing and Bridging (IRB) interface is configured and it is mapped to a VPLS instance or a Bridge-Domain, certain network events at Customer Edge (CE) device may cause memory leak in the MPC which can cause an out of memory and MPC restarts. When this issue occurs, there will be temporary traffic interruption until the MPC is restored. An administrator can use the following CLI command to monitor the status of memory usage level of the MPC: user@device> show system resource-monitor fpc FPC Resource Usage Summary Free Heap Mem Watermark : 20 % Free NH Mem Watermark : 20 % Free Filter Mem Watermark : 20 % * - Watermark reached Slot # % Heap Free RTT Average RTT 1 87 PFE # % ENCAP mem Free % NH mem Free % FW mem Free 0 NA 88 99 1 NA 89 99	2021-01-15	5	CVE-2021-0202 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	When the issue is occurring, the value of “% NH mem Free” will go down until the MPC restarts. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX Series, EX9200 Series: 17.3R3-S8; 17.4R3-S2; 18.2R3-S4, 18.2R3-S5; 18.3R3-S2, 18.3R3-S3; 18.4 versions starting from 18.4R3-S1 and later versions prior to 18.4R3-S6; 19.2 versions starting from 19.2R2 and later versions prior to 19.2R3-S1; 19.4 versions starting from 19.4R2 and later versions prior to 19.4R2-S3, 19.4R3; 20.2 versions starting from 20.2R1 and later versions prior to 20.2R1-S3, 20.2R2. This issue does not affect Juniper Networks Junos OS: 18.1, 19.1, 19.3, 20.1.			
juniper -- junos	On Juniper Networks EX and QFX5K Series platforms configured with Redundant Trunk Group (RTG), Storm Control profile applied on the RTG interface might not take affect when it reaches the threshold condition. Storm Control enables the device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. Note: this issue does not affect EX2200, EX3300, EX4200, and EX9200 Series. This	2021-01-15	4.3	CVE-2021-0203 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue affects Juniper Networks Junos OS on EX Series and QFX5K Series: 15.1 versions prior to 15.1R7-S7; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2.			
juniper -- junos	When the "Intrusion Detection Service" (IDS) feature is configured on Juniper Networks MX series with a dynamic firewall filter using IPv6 source or destination prefix, it may incorrectly match the prefix as /32, causing the filter to block unexpected traffic. This issue affects only IPv6 prefixes when used as source and destination. This issue affects MX Series devices using MS-MPC, MS-MIC or MS-SPC3 service cards with IDS service configured. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S10 on MX Series; 17.4 versions prior to 17.4R3-S3 on MX Series; 18.1 versions prior to 18.1R3-S11 on MX Series; 18.2 versions prior to 18.2R3-S6 on MX Series;	2021-01-15	4.3	CVE-2021-0205 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	18.3 versions prior to 18.3R3-S4 on MX Series; 18.4 versions prior to 18.4R3-S6 on MX Series; 19.1 versions prior to 19.1R2-S2, 19.1R3-S3 on MX Series; 19.2 versions prior to 19.2R3-S1 on MX Series; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1 on MX Series; 19.4 versions prior to 19.4R3 on MX Series; 20.1 versions prior to 20.1R2 on MX Series; 20.2 versions prior to 20.2R2 on MX Series;			
juniper -- junos_evolved	In Juniper Networks Junos OS Evolved an attacker sending certain valid BGP update packets may cause Junos OS Evolved to access an uninitialized pointer causing RPD to core leading to a Denial of Service (DoS). Continued receipt of these types of valid BGP update packets will cause an extended Denial of Service condition. RPD will require a restart to recover. An indicator of compromise is to see if the file rpd.re exists by issuing the command: show system core-dumps This issue affects: Juniper Networks Junos OS Evolved 19.4 versions prior to 19.4R2-S2-EVO; 20.1 versions prior to 20.1R1-S2-EVO, 20.1R2-S1-EVO. This issue does not affect Junos OS.	2021-01-15	5.7	CVE-2021-0209 CONFIRM
libsdl -- sdl	SDL (Simple DirectMedia Layer) through 2.0.12 has a heap-based buffer over-read in	2021-01-19	6.8	CVE-2020-14410

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Blit_3or4_to_3or4__inversed_rgb in video/SDL_blit_N.c via a crafted .BMP file.			MISC MISC
libsdl -- sdl	SDL (Simple DirectMedia Layer) through 2.0.12 has an Integer Overflow (and resultant SDL_memcpy heap corruption) in SDL_BlitCopy in video/SDL_blit_copy.c via a crafted .BMP file.	2021-01-19	6.8	CVE-2020-14409 MISC MISC
malwarebytes -- malwarebytes	An issue was discovered in Malwarebytes before 4.0 on macOS. A malicious application was able to perform a privileged action within the Malwarebytes launch daemon. The privileged service improperly validated XPC connections by relying on the PID instead of the audit token. An attacker can construct a situation where the same PID is used for running two different programs at different times, by leveraging a race condition during crafted use of posix_spawn.	2021-01-15	6.9	CVE-2020-25533 MISC
mantisbt -- source_integration	An issue was discovered in the Source Integration plugin before 2.4.1 for MantisBT. An attacker can gain access to the Summary field of private Issues (either marked as Private, or part of a private Project), if they are attached to an existing Changeset. The information is visible on the view.php page, as well as on the	2021-01-18	5	CVE-2020-36192 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	list.php page (a pop-up on the Affected Issues id hyperlink). Additionally, if the attacker has "Update threshold" in the plugin's configuration (set to the "updater" access level by default), then they can link any Issue to a Changeset by entering the Issue's Id, even if they do not have access to it.			
medintux -- medintux	Reflected XSS in Medintux v2.16.000 CCAM.php by manipulating the mot1 parameter can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.	2021-01-20	4.3	CVE-2020-19361 MISC MISC MISC
misp -- misp	The default setting of MISP 2.4.136 did not enable the requirements (aka require_password_confirmation) to provide the previous password when changing a password.	2021-01-19	6.4	CVE-2021-25323 MISC
misp -- misp	MISP 2.4.136 has XSS via a crafted URL to the app/View/Elements/global_menu.ctp user homepage favourite button.	2021-01-19	4.3	CVE-2021-3184 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
misp -- misp	MISP 2.4.136 has XSS via galaxy cluster element values to app/View/GalaxyElements/ajax/index.ctp. Reference types could contain javascript: URLs.	2021-01-19	4.3	CVE-2021-25325 MISC
misp -- misp	MISP 2.4.136 has Stored XSS in the galaxy cluster view via a cluster name to app/View/GalaxyClusters/view.ctp.	2021-01-19	4.3	CVE-2021-25324 MISC
nagios -- log_server	Nagios Log Server 2.1.7 contains a cross-site scripting (XSS) vulnerability in /nagioslogserver/configure/create_snapshot through the snapshot_name parameter, which may impact users who open a maliciously crafted link or third-party web page.	2021-01-20	4.3	CVE-2020-25385 MISC
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is an issue involving YAML parsing which can lead to post-auth remote code execution. In order to parse and process YAML files, OneDev uses SnakeYaml which by default (when not using `SafeConstructor`) allows the instantiation of arbitrary classes. We can leverage that to run arbitrary code by instantiating classes such as	2021-01-15	6.5	CVE-2021-21249 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`javax.script.ScriptEngineManager` and using `URLClassLoader` to load the script engine provider, resulting in the instantiation of a user controlled class. For a full example refer to the referenced GHSA. This issue was addressed in 4.0.3 by only allowing certain known classes to be deserialized			
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3 there is a critical "zip slip" vulnerability. This issue may lead to arbitrary file write. The KubernetesResource REST endpoint untars user controlled data from the request body using TarUtils. TarUtils is a custom library method leveraging Apache Commons Compress. During the untar process, there are no checks in place to prevent an untarred file from traversing the file system and overriding an existing file. For a successful exploitation, the attacker requires a valid __JobToken__ which may not be possible to get without using any of the other reported vulnerabilities. But this should be considered a vulnerability in `io.onedev.commons.utils.TarUtils` since it lives in a different artifact and can affect other projects using it. This issue was addressed in 4.0.3 by validating paths in tar archive to only allow them to be in specified folder when extracted.	2021-01-15	6.5	CVE-2021-21251 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is a critical vulnerability involving the build endpoint parameters. InputSpec is used to define parameters of a Build spec. It does so by using dynamically generated Groovy classes. A user able to control job parameters can run arbitrary code on OneDev's server by injecting arbitrary Groovy code. The ultimate result is in the injection of a static constructor that will run arbitrary code. For a full example refer to the referenced GHSA. This issue was addressed in 4.0.3 by escaping special characters such as quote from user input.	2021-01-15	6.5	CVE-2021-21248 MISC CONFIRM
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, the REST UserResource endpoint performs a security check to make sure that only administrators can list user details. However for the `/users/{id}` endpoint there are no security checks enforced so it is possible to retrieve arbitrary user details including their Access Tokens! These access tokens can be used to access the API or clone code in the build spec via the HTTP(S) protocol. It has permissions to all projects accessible by the user account. This issue may lead to `Sensitive data leak` and leak the Access Token which can be used to impersonate the administrator or any other users. This	2021-01-15	5	CVE-2021-21246 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue was addressed in 4.0.3 by removing user info from restful api.			
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, there is a critical vulnerability which may lead to arbitrary file read. When BuildSpec is provided in XML format, the spec is processed by XmlBuildSpecMigrator.migrate(buildSpecString); which processes the XML document without preventing the expansion of external entities. These entities can be configured to read arbitrary files from the file system and dump their contents in the final XML document to be migrated. If the files are dumped in properties included in the YAML file, it will be possible for an attacker to read them. If not, it is possible for an attacker to exfiltrate the contents of these files Out Of Band. This issue was addressed in 4.0.3 by ignoring ENTITY instructions in xml file.	2021-01-15	4	CVE-2021-21250 MISC CONFIRM
onedev_project -- onedev	OneDev is an all-in-one devops platform. In OneDev before version 4.0.3, the application's BasePage registers an AJAX event listener (`AbstractPostAjaxBehavior`) in all pages other than the login page. This listener decodes and deserializes the `data` query parameter. We can access this listener by submitting a POST request to any page. This issue	2021-01-15	6.5	CVE-2021-21247 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may lead to `post-auth RCE` This endpoint is subject to authentication and, therefore, requires a valid user to carry on the attack. This issue was addressed in 4.0.3 by encrypting serialization payload with secrets only known to server.			
open-emr -- openemr	OpenEMR 5.0.1 allows an authenticated attacker to upload and execute malicious PHP scripts through /controller.php.	2021-01-20	6.5	CVE-2020-19364 MISC
opendesign -- drawings_software_development_kit	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A stack-based buffer overflow vulnerability exists when the recover operation is run with malformed .DXF and .DWG files. This can allow attackers to cause a crash potentially enabling a denial of service attack (Crash, Exit, or Restart) or possible code execution.	2021-01-18	6.8	CVE-2021-25178 MISC
opendesign -- drawings_software_development_kit	An issue was discovered in Open Design Alliance Drawings SDK before 2021.12. A memory corruption vulnerability exists when reading malformed DGN files. It can allow attackers to cause a crash, potentially enabling denial of service (Crash, Exit, or Restart).	2021-01-18	4.3	CVE-2021-25174 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opendesign -- drawings_software_development_kit	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A NULL pointer dereference exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). This is issue 1 of 3.	2021-01-18	4.3	CVE-2021-25175 MISC
opendesign -- drawings_software_development_kit	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A NULL pointer dereference exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). This is issue 2 of 3.	2021-01-18	4.3	CVE-2021-25176 MISC
opendesign -- drawings_software_development_kit	An issue was discovered in Open Design Alliance Drawings SDK before 2021.11. A NULL pointer dereference exists when rendering malformed .DXF and .DWG files. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart). This is issue 3 of 3.	2021-01-18	4.3	CVE-2021-25177 MISC
oracle -- business_intelligence	Vulnerability in the Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Dashboards). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0,	2021-01-20	4.9	CVE-2021-2003 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).			
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: BI Platform Security). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence	2021-01-20	4.3	CVE-2021-2005 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N).			
oracle -- business_intelligence_publisher	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	2021-01-20	6.5	CVE-2021-2013 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Report). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2021-01-20	5.5	CVE-2021-1997 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2021-01-20	4	CVE-2021-2032 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 5.7.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2014 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2020 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2012 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2001 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2009 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2002 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2021-01-20	4	CVE-2021-2019 MISC
oracle -- mysql	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2021-01-20	4.3	CVE-2021-2007 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2016 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2072 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	4.9	CVE-2021-2088 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2036 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2081 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2122 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2070 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2060 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.3	CVE-2021-2006 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.3	CVE-2021-2022 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.3	CVE-2021-2038 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.3	CVE-2021-2056 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.3	CVE-2021-2061 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).	2021-01-20	5.5	CVE-2021-1998 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2058 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2055 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2046 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2031 MISC

Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2076 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	4.9	CVE-2021-2087 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L).	2021-01-20	4.9	CVE-2021-2010 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2021 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2024 MISC
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2028 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2021-01-20	6.8	CVE-2021-2030 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	2021-01-20	4	CVE-2021-1995 MISC
owncloud -- owncloud	ownCloud (Core) before 10.5 allows XSS in login page 'forgot password.'	2021-01-15	4.3	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				16255 MISC MISC
php -- archive_tar	Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.	2021-01-18	5	CVE-2020-36193 MISC
pixelimity -- pixelimity	Pixelimity 1.0 has cross-site request forgery via the admin/setting.php data [Password] parameter.	2021-01-19	6	CVE-2020-23522 MISC
presstigers -- simple_board_job	Directory traversal vulnerability in class-simple_job_board_resume_download_handler.php in the Simple Board Job plugin 2.9.3 and earlier for WordPress allows remote attackers to read arbitrary files via the sjb_file parameter to wp-admin/post.php.	2021-01-15	4	CVE-2020-35749 MISC
quali -- cloudshell	An issue was discovered in Quali CloudShell 9.3. An XSS vulnerability in the login page allows an attacker to craft a URL, with a constructor.constructor substring in the username field, that executes a payload when the user visits the /Account/Login page.	2021-01-17	4.3	CVE-2020-15864 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sooil -- anydana-a_firmware	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, a hard-coded physician PIN in the physician menu of the insulin pump allows attackers with physical access to change insulin therapy settings.	2021-01-19	4.6	CVE-2020-27256 MISC
stockdio -- stockdio_historical_chart	The Stockdio Historical Chart plugin before 2.8.1 for WordPress is affected by Cross Site Scripting (XSS) via stockdio_chart_historical-wp.js in wp-content/plugins/stockdio-historical-chart/assets/ because the origin of a postMessage() event is not validated. The stockdio_eventer function listens for any postMessage event. After a message event is sent to the application, this function sets the "e" variable as the event and checks that the types of the data and data.method are not undefined (empty) before proceeding to eval the data.method received from the postMessage. However, on a different website. JavaScript code can call window.open for the vulnerable WordPress instance and do a postMessage(msg,'*') for that object.	2021-01-19	4.3	CVE-2020-28707 MISC MISC CONFIRM
tufin -- securechange	Tufin SecureChange prior to R19.3 HF3 and R20-1 HF1 are vulnerable to stored XSS. The successful exploitation requires admin privileges (for storing the XSS payload itself), and can exploit (be triggered by) unauthenticated users. All TOS versions with	2021-01-20	4.3	CVE-2020-13133 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SecureChange deployments prior to R19.3 HF3 and R20-1 HF1 are affected. Vulnerabilities were fixed in R19.3 HF3 and R20-1 HF1			
vtiger -- vtiger_crm	Vtiger CRM v7.2.0 allows an attacker to display hidden files, list directories by using /libraries and /layout directories.	2021-01-20	4.3	CVE-2020-19363 MISC MISC MISC
vtiger -- vtiger_crm	Reflected XSS in Vtiger CRM v7.2.0 in vtigercrm/index.php? through the view parameter can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.	2021-01-20	4.3	CVE-2020-19362 MISC MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI (v4.2 Series) versions prior to v4.2.3 allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-01-19	4.3	CVE-2021-20619 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zohocorp -- manageengine_applications_manager	Zoho ManageEngine Applications Manager before 14 build 14880 allows an authenticated SQL Injection via a crafted Alarmview request.	2021-01-19	6.5	CVE-2020-27733 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aia -- my_aia_sg	The My AIA SG application 1.2.6 for Android allows attackers to obtain user credentials via logcat because of excessive logging.	2021-01-19	2.1	CVE-2020-29598 MISC MISC
flatcore -- flatcore	An issue was discovered in flatCore before 2.0.0 build 139. A stored XSS vulnerability was identified in the prefs_smtp_psw HTTP request body parameter for the acp interface. An admin user can inject malicious client-side script into the affected parameter without any form of input sanitization. The injected payload	2021-01-15	3.5	CVE-2021-23836 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	will be executed in the browser of a user whenever one visits the affected module page.			
flatcore -- flatcore	An issue was discovered in flatCore before 2.0.0 build 139. A reflected XSS vulnerability was identified in the media_filter HTTP request body parameter for the acp interface. The affected parameter accepts malicious client-side script without proper input sanitization. For example, a malicious user can leverage this vulnerability to steal cookies from a victim user and perform a session-hijacking attack, which may then lead to unauthorized access to the site.	2021-01-15	3.5	CVE-2021-23838 MISC MISC MISC
foliovision -- fv_flowplayer_video_player	Cross-site scripting (XSS) vulnerability in models/list-table.php in the FV Flowplayer Video Player plugin before 7.4.37.727 for WordPress allows remote authenticated users to inject arbitrary web script or HTML via the fv_wp_fvvideoplayer_src JSON field in the data parameter.	2021-01-15	3.5	CVE-2020-35748 MISC MISC
ibm -- aix	IBM AIX 7.1, 7.2 and AIX VIOS 3.1 could allow a local user to exploit a vulnerability in the gencore user command to create arbitrary files in any directory. IBM X-Force ID: 190911.	2021-01-20	2.1	CVE-2020-4887 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- planning_analytics	IBM Planning Analytics 2.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 190834.	2021-01-19	2.1	CVE-2020-4871 XF CONFIRM
juniper -- junos	On Juniper Networks Junos EX series, QFX Series and SRX branch series devices, a memory leak occurs every time the 802.1X authenticator port interface flaps which can lead to other processes, such as the pfex process, responsible for packet forwarding, to crash and restart. An administrator can use the following CLI command to monitor the status of memory consumption: user@device> show task memory detail Please refer to https://kb.juniper.net/KB31522 for details. This issue affects Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D54; 15.1X49 versions prior to 15.1X49-D240 ; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10 ; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2.	2021-01-15	2.9	CVE-2021-0215 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This issue does not affect Juniper Networks Junos OS 12.3, 15.1.			
juniper -- junos	An improper input validation vulnerability in the Routing Protocol Daemon (RPD) service of Juniper Networks Junos OS allows an attacker to send a malformed RSVP packet when bidirectional LSPs are in use, which when received by an egress router crashes the RPD causing a Denial of Service (DoS) condition. Continued receipt of the packet will sustain the Denial of Service. This issue affects: Juniper Networks Junos OS: All versions prior to 17.3R3-S10 except 15.1X49-D240 for SRX series; 17.4 versions prior to 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S4; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R1-S8, 18.4R2-S6, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R3-S3; 19.2 versions prior to 19.2R3; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3-S1; 20.1 versions prior to 20.1R1-S4, 20.1R2; 15.1X49 versions prior to 15.1X49-D240 on SRX Series. Juniper Networks Junos OS Evolved: 19.3 versions prior to 19.3R2-S5-EVO; 19.4 versions prior to 19.4R2-S2-EVO; 20.1 versions prior to 20.1R1-S4-EVO.	2021-01-15	3.3	CVE-2021-0208 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
juniper -- junos	A vulnerability in processing of certain DHCP packets from adjacent clients on EX Series and QFX Series switches running Juniper Networks Junos OS with DHCP local/relay server configured may lead to exhaustion of DMA memory causing a Denial of Service (DoS). Over time, exploitation of this vulnerability may cause traffic to stop being forwarded, or to crashing of the fxpc process. When Packet DMA heap utilization reaches 99%, the system will become unstable. Packet DMA heap utilization can be monitored through the following command: user@junos# request pfe execute target fpc0 timeout 30 command "show heap" ID Base Total(b) Free(b) Used(b) % Name -- ---------- ----------- ----------- ----------- --- ----------- 0 213301a8 536870488 387228840 149641648 27 Kernel 1 91800000 8388608 3735120 4653488 55 DMA 2 92000000 75497472 74452192 1045280 1 PKT DMA DESC 3 d330000 335544320 257091400 78452920 23 Bcm_sdk 4 96800000 184549376 2408 184546968 99 Packet DMA <--- 5 903fffe0 20971504 20971504 0 0 Blob An indication of the issue occurring may be observed through the following log messages: Dec 10 08:07:00.124 2020 hostname fpc0 brcm_pkt_buf_alloc:523 (buf alloc) failed allocating packet buffer Dec 10 08:07:00.126 2020 hostname fpc0 (buf alloc) failed allocating packet buffer Dec 10 08:07:00.128 2020 hostname fpc0	2021-01-15	3.3	CVE-2021-0217 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	brcm_pkt_buf_alloc:523 (buf alloc) failed allocating packet buffer Dec 10 08:07:00.130 2020 hostnameC fpc0 (buf alloc) failed allocating packet buffer This issue affects Juniper Networks Junos OS on EX Series and QFX Series: 17.4R3 versions prior to 17.4R3-S3; 18.1R3 versions between 18.1R3-S6 and 18.1R3-S11; 18.2R3 versions prior to 18.2R3-S6; 18.3R3 versions prior to 18.3R3-S4; 18.4R2 versions prior to 18.4R2-S5; 18.4R3 versions prior to 18.4R3-S6; 19.1 versions between 19.1R2 and 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2. Junos OS versions prior to 17.4R3 are unaffected by this vulnerability.			
mcafee -- mcafee_agent	Missing Authorization vulnerability in McAfee Agent (MA) for Windows prior to 5.7.1 allows local users to block McAfee product updates by manipulating a directory used by MA for temporary files. The product would continue to function with out-of-date detection files.	2021-01-18	2.1	CVE-2020-7343 CONFIRM
oracle -- agile_engineering_data_management	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are	2021-01-20	3.5	CVE-2021-1996 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).			
oracle -- database_server	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having SYS Account privilege with network access via Oracle Net to compromise Unified Audit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Unified Audit accessible data. CVSS 3.1 Base Score 2.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N).	2021-01-20	3.5	CVE-2021-2000 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 4.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N).	2021-01-20	2.1	CVE-2021-1993 MISC
oracle -- enterprise_manager_ops_center	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: RAS subsystems). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle ZFS Storage Appliance Kit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access	2021-01-20	1.2	CVE-2021-1999 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to critical data or all Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:N).			
oracle -- mysql	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	2021-01-20	2.1	CVE-2021-2042 MISC
rocketgenius -- gravityforms	Multiple stored HTML injection vulnerabilities in the "poll" and "quiz" features in an additional paid add-on of Rocketgenius Gravity Forms before 2.4.21 allows remote attackers to inject arbitrary HTML code via poll or quiz answers. This code is interpreted by users in a privileged role (Administrator, Editor, etc.).	2021-01-20	3.5	CVE-2020-27851 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rocketgenius -- gravityforms	A stored Cross-Site Scripting (XSS) vulnerability in the survey feature in Rocketgenius Gravity Forms before 2.4.21 allows remote attackers to inject arbitrary web script or HTML via a textarea field. This code is interpreted by users in a privileged role (Administrator, Editor, etc.).	2021-01-20	3.5	CVE-2020-27852 MISC
rocketgenius -- gravityforms	A stored Cross-Site Scripting (XSS) vulnerability in forms import feature in Rocketgenius Gravity Forms before 2.4.21 allows remote attackers to inject arbitrary web script or HTML via the import of a GF form. This code is interpreted by users in a privileged role (Administrator, Editor, etc.).	2021-01-20	3.5	CVE-2020-27850 MISC
solarwinds -- web_help_desk	SolarWinds Web Help Desk 12.7.0 allows XSS via a Schedule Name.	2021-01-15	3.5	CVE-2019-16961 MISC MISC MISC
sooil -- anydana-a	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, an information disclosure vulnerability in the communication protocol of the insulin pump and its AnyDana-i and AnyDana-A	2021-01-19	3.3	CVE-2020-27258 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mobile applications allows unauthenticated attackers to extract the pump's keypad lock PIN via Bluetooth Low Energy.			
sooil -- anydana-a_firmware	SOOIL Developments CoLtd DiabecareRS, AnyDana-i, AnyDana-A, The communication protocol of the insulin pump and AnyDana-i,AnyDana-A mobile apps doesn't use adequate measures to authenticate the pump before exchanging keys, which allows unauthenticated, physically proximate attackers to eavesdrop the keys and spoof the pump via BLE.	2021-01-19	2.9	CVE-2020-27272 MISC
sooil -- anydana-a_firmware	SOOIL Developments Co Ltd DiabecareRS,AnyDana-i & AnyDana-A, the communication protocol of the insulin pump and its AnyDana-i & AnyDana-A mobile apps doesn't use adequate measures to authenticate the communicating entities before exchanging keys, which allows unauthenticated, physically proximate attackers to eavesdrop the authentication sequence via Bluetooth Low Energy.	2021-01-19	2.9	CVE-2020-27276 MISC
sooil -- anydana-a_firmware	SOOIL Developments CoLtd DiabecareRS, AnyDana-i ,AnyDana-A, communication protocol of the insulin pump & AnyDana-i,AnyDana-A mobile apps doesnt use adequate measures to protect encryption keys in	2021-01-19	2.9	CVE-2020-27270 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	transit which allows unauthenticated physically proximate attacker to sniff keys via (BLE).			
sooil -- anydana-a_firmware	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, the communication protocol of the insulin pump and its AnyDana-i and AnyDana-A mobile applications lacks replay protection measures, which allows unauthenticated, physically proximate attackers to replay communication sequences via Bluetooth Low Energy.	2021-01-19	2.9	CVE-2020-27269 MISC
sooil -- anydana-a_firmware	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, a client-side control vulnerability in the insulin pump and its AnyDana-i and AnyDana-A mobile applications allows physically proximate attackers to bypass user authentication checks via Bluetooth Low Energy.	2021-01-19	3.3	CVE-2020-27266 MISC
sooil -- anydana-a_firmware	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, the communication protocol of the insulin pump and its AnyDana-i and AnyDana-A mobile applications use deterministic keys, which allows unauthenticated, physically proximate attackers to brute-force the keys via Bluetooth Low Energy.	2021-01-19	3.3	CVE-2020-27264 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sooil -- anydana-a_firmware	In SOOIL Developments Co., Ltd Diabecare RS, AnyDana-i and AnyDana-A, a client-side control vulnerability in the insulin pump and its AnyDana-i and AnyDana-A mobile applications allows physically proximate attackers to bypass checks for default PINs via Bluetooth Low Energy.	2021-01-19	3.3	CVE-2020-27268 MISC
tufin -- securechange	Tufin SecureChange prior to R19.3 HF3 and R20-1 HF1 are vulnerable to stored XSS. The successful exploitation requires admin privileges (for storing the XSS payload itself), and can exploit (be triggered by) admin users. All TOS versions with SecureChange deployments prior to R19.3 HF3 and R20-1 HF1 are affected. Vulnerabilities were fixed in R19.3 HF3 and R20-1 HF1.	2021-01-20	3.5	CVE-2020-13134 MISC MISC
xwiki -- xwiki	XWiki 12.10.2 allows XSS via an SVG document to the upload feature of the comment section.	2021-01-20	3.5	CVE-2021-3137 MISC