National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 31 Jan 2022 Vol. 09 No. 02

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
android-gif-drawable_project					
android-gif-drawable					
N/A	19-Jan-22	5	decoding.c in android-gif-drawable before 1.2.24 does not limit the maximum length of a comment, leading to denial of service. **CVE ID : CVE-2022-23435**	https://github.com/koral--/android-gif-drawable/commit/9f0f0c89e6fa38548163771feeb4bde84b828887, https://github.com/koral--/android-gif-drawable/compare/v1.2.23...v1.2.24	A-AND-ANDR-030222/1
Apache					
chainsaw					
Deserialization of Untrusted Data	18-Jan-22	10	CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists. **CVE ID : CVE-2022-23307**	https://lists.apache.org/thread/rg4yyc89vs3dw6kpy3r92xop9loywyhh, https://logging.apache.org/log4j/1.2/index.html	A-APA-CHAI-030222/2
log4j					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	18-Jan-22	6	JMSSink in all versions of Log4j 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration or if the configuration references an LDAP service the attacker has access to. The attacker can provide a TopicConnectionFactoryBindingName configuration causing JMSSink to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-4104. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions. **CVE ID : CVE-2022-23302**	https://lists.apache.org/thread/bsr3l5qz4g0myrjhy9h67bcxodpkwj4w, https://logging.apache.org/log4j/1.2/index.html	A-APA-LOG4-030222/3
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jan-22	6.8	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged	https://lists.apache.org/thread/pt6lh3pbsvxqlwlp4c5l798dv2hkc85y, https://logging.apache.org/log4j/1.2/index.html	A-APA-LOG4-030222/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowing unintended SQL queries to be executed. Note this issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions. **CVE ID : CVE-2022-23305**		
Deserialization of Untrusted Data	18-Jan-22	10	CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists. **CVE ID : CVE-2022-23307**	https://lists.apache.org/thread/rg4yyc89vs3dw6kpy3r92xop9loywyhh, https://logging.apache.org/log4j/1.2/index.html	A-APA-LOG4-030222/5
shardingsphere_elasticjob-ui					
Exposure of Sensitive Information to an Unauthorized Actor	20-Jan-22	4	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache ShardingSphere ElasticJob-UI allows an attacker who has guest account to do privilege escalation. This issue affects	https://lists.apache.org/thread/qpdsm936n9bhksb0rzn6bq1h7ord2nm6	A-APA-SHAR-030222/6

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Apache ShardingSphere ElasticJob-UI Apache ShardingSphere ElasticJob-UI 3.x version 3.0.0 and prior versions. **CVE ID : CVE-2022-22733**		
Broadcom					
netmaster_file_transfer_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	4.3	NetMaster 12.2 Network Management for TCP/IP and NetMaster File Transfer Management contain a XSS (Cross-Site Scripting) vulnerability in ReportCenter UI due to insufficient input validation that could potentially allow an attacker to execute code on the affected machine. **CVE ID : CVE-2022-23083**	https://support.broadcom.com/external/content/security-advisories/NetMaster-12.2-ReportCenter-Vulnerability-CVE-2022-23083/20049	A-BRO-NETM-030222/7
netmaster_network_management_for_tcp\\/ip					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	4.3	NetMaster 12.2 Network Management for TCP/IP and NetMaster File Transfer Management contain a XSS (Cross-Site Scripting) vulnerability in ReportCenter UI due to insufficient input validation that could potentially allow an attacker to execute code on the affected machine. **CVE ID : CVE-2022-23083**	https://support.broadcom.com/external/content/security-advisories/NetMaster-12.2-ReportCenter-Vulnerability-CVE-2022-23083/20049	A-BRO-NETM-030222/8
Buffercode					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
random_banner					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	3.5	The Random Banner WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the category parameter found in the ~/include/models/model.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2022-0210**	N/A	A-BUF-RAND-030222/9
Codeigniter					
codeigniter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-22	4.3	CodeIgniter4 is the 4.x branch of CodeIgniter, a PHP full-stack web framework. A cross-site scripting (XSS) vulnerability was found in `API\ResponseTrait` in Codeigniter4 prior to version 4.1.8. Attackers can do XSS attacks if a potential victim is using `API\ResponseTrait`. Version 4.1.8 contains a patch for this vulnerability. There are two potential workarounds available. Users may avoid using `API\ResponseTrait` or `ResourceController` Users	https://codeigniter4.github.io/userguide/incoming/routing.html#use-defined-routes-only, https://github.com/codeigniter4/CodeIgniter4/security/advisories/GHSA-7528-7jg5-6g62	A-COD-CODE-030222/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may also disable Auto Route and use defined routes only. **CVE ID : CVE-2022-21715**		
conda_loguru_project					
conda_loguru					
Improper Privilege Management	25-Jan-22	4	Improper Privilege Management in Conda loguru prior to 0.5.3. **CVE ID : CVE-2022-0338**	https://huntr.dev/bounties/359bea50-2bc6-426a-b2f9-175d401b1ed0, https://github.com/delgan/loguru/commit/ea39375e62f9b8f18e2ca798a5c0fb8c972b7eaa	A-CON-COND-030222/11
contribsys					
sidekiq					
Allocation of Resources Without Limits or Throttling	21-Jan-22	5	In api.rb in Sidekiq before 6.4.0, there is no limit on the number of days when requesting stats for the graph. This overloads the system, affecting the Web UI, and makes it unavailable to users. **CVE ID : CVE-2022-23837**	https://github.com/mperham/sidekiq/commit/7785ac1399f1b28992adb56055f6acd88fd1d956	A-CON-SIDE-030222/12
craterapp					
crater					
Unrestricted Upload of File with Dangerous	17-Jan-22	6	Unrestricted Upload of File with Dangerous Type in GitHub repository crater-invoice/crater prior to 6.0.	https://huntr.dev/bounties/19f3e5f7-b419-44b1-	A-CRA-CRAT-030222/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			**CVE ID : CVE-2022-0242**	9c37-7e4404cbec94, https://github.com/crater-invoice/crater/commit/dcb3ddecb9f4cde622cc42c51a2760747797624f	
Dell					
emc_appsync					
Session Fixation	21-Jan-22	5.8	DELL EMC AppSync versions 3.9 to 4.3 use GET request method with sensitive query strings. An Adjacent, unauthenticated attacker could potentially exploit this vulnerability, and hijack the victim session. **CVE ID : CVE-2022-22551**	https://www.dell.com/support/kbdoc/000195377	A-DEL-EMC_-030222/14
Improper Restriction of Rendered UI Layers or Frames	21-Jan-22	5.8	Dell EMC AppSync versions 3.9 to 4.3 contain a clickjacking vulnerability in AppSync. A remote unauthenticated attacker could potentially exploit this vulnerability to trick the victim into executing state changing operations. **CVE ID : CVE-2022-22552**	https://www.dell.com/support/kbdoc/000195377	A-DEL-EMC_-030222/15
Improper Restriction of Excessive Authentication Attempts	21-Jan-22	7.5	Dell EMC AppSync versions 3.9 to 4.3 contain an Improper Restriction of Excessive Authentication Attempts Vulnerability that can be exploited from UI and	https://www.dell.com/support/kbdoc/000195377	A-DEL-EMC_-030222/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CLI. An adjacent unauthenticated attacker could potentially exploit this vulnerability, leading to password brute-forcing. Account takeover is possible if weak passwords are used by users. **CVE ID : CVE-2022-22553**		
emc_system_update					
Insufficiently Protected Credentials	24-Jan-22	2.1	Dell EMC System Update, version 1.9.2 and prior, contain an Unprotected Storage of Credentials vulnerability. A local attacker with user privleges could potentially exploit this vulnerability leading to the disclosure of user passwords. **CVE ID : CVE-2022-22554**	https://www.dell.com/support/kbdoc/000195007	A-DEL-EMC_-030222/17
elfspirit_project					
elfspirit					
Out-of-bounds Read	24-Jan-22	5.8	elfspirit is an ELF static analysis and injection framework that parses, manipulates, and camouflages ELF files. When analyzing the ELF file format in versions prior to 1.1, there is an out-of-bounds read bug, which can lead to application crashes or information leakage. By constructing a special format ELF file, the information of any address can be leaked. elfspirit version 1.1 contains a patch for this issue.	https://github.com/liyansong2018/elfspirit/commit/c5b0f5a9a24f2451bbeda4751d67633bc375e608, https://github.com/liyansong2018/elfspirit/security/advisories/GHSA-jr8h-2657-m68r	A-ELF-ELFS-030222/18

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21711		
epub2txt_project					
epub2txt					
Out-of-bounds Write	23-Jan-22	6.8	xhtml_translate_entity in xhtml.c in epub2txt (aka epub2txt2) through 2.02 allows a stack-based buffer overflow via a crafted EPUB document. **CVE ID : CVE-2022-23850**	N/A	A-EPU-EPUB-030222/19
exiftool_project					
exiftool					
N/A	25-Jan-22	7.5	lib/Image/ExifTool.pm in ExifTool before 12.38 mishandles a $file =~ /\|$/ check. **CVE ID : CVE-2022-23935**	https://github.com/exiftool/exiftool/commit/74dbab1d2766d6422bb05b033ac6634bf8d1f582	A-EXI-EXIF-030222/20
expresstech					
quiz_and_survey_master					
Cross-Site Request Forgery (CSRF)	17-Jan-22	6.8	Cross-site request forgery (CSRF) vulnerability in Quiz And Survey Master versions prior to 7.3.7 allows a remote attacker to hijack the authentication of administrators and conduct arbitrary operations via a specially crafted web page. **CVE ID : CVE-2022-0180**	https://wordpress.org/plugins/quiz-master-next/	A-EXP-QUIZ-030222/21
Improper Neutralization of Input During Web Page	17-Jan-22	4.3	Reflected cross-site scripting vulnerability in Quiz And Survey Master versions prior to 7.3.7 allows a remote attacker to inject an arbitrary	https://wordpress.org/plugins/quiz-master-next/	A-EXP-QUIZ-030222/22

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			script via unspecified vectors. **CVE ID : CVE-2022-0181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-22	3.5	Stored cross-site scripting vulnerability in Quiz And Survey Master versions prior to 7.3.7 allows a remote authenticated attacker to inject an arbitrary script via an website that uses Quiz And Survey Master. **CVE ID : CVE-2022-0182**	https://wordpress.org/plugins/quiz-master-next/	A-EXP-QUIZ-030222/23
getgrav					
grav					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist getgrav/grav prior to 1.7.28. **CVE ID : CVE-2022-0268**	https://github.com/getgrav/grav/commit/6f2fa9311afb9ecd34030dec2aff7b39e9e7e735, https://huntr.dev/bounties/67085545-331e-4469-90f3-a1a46a078d39	A-GET-GRAV-030222/24
Gitlab					
gitlab					
Improper Privilege Management	18-Jan-22	5	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab is configured in a way that it doesn't ignore	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0090.json	A-GIT-GITL-030222/25

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			replacement references with git sub-commands, allowing a malicious user to spoof the contents of their commits in the UI. **CVE ID : CVE-2022-0090**		
Exposure of Sensitive Information to an Unauthorized Actor	18-Jan-22	4	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. GitLab allows a user with an expired password to access sensitive information through RSS feeds. **CVE ID : CVE-2022-0093**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0093.json	A-GIT-GITL-030222/26
Improper Input Validation	18-Jan-22	4	An issue has been discovered affecting GitLab versions prior to 14.4.5, between 14.5.0 and 14.5.3, and between 14.6.0 and 14.6.1. Gitlab's Slack integration is incorrectly validating user input and allows to craft malicious URLs that are sent to slack. **CVE ID : CVE-2022-0124**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0124.json	A-GIT-GITL-030222/27
Improper Privilege Management	18-Jan-22	4	An issue has been discovered in GitLab affecting all versions starting from 12.0 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not verifying that a maintainer of a project had the right access to import members from a target project.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0125.json	A-GIT-GITL-030222/28

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0125		
N/A	18-Jan-22	5	An issue has been discovered in GitLab affecting all versions starting from 12.10 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was not correctly handling requests to delete existing packages which could result in a Denial of Service under specific conditions. **CVE ID : CVE-2022-0151**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0151.json	A-GIT-GITL-030222/29
Missing Authorization	18-Jan-22	4	An issue has been discovered in GitLab affecting all versions starting from 13.10 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to unauthorized access to some particular fields through the GraphQL API. **CVE ID : CVE-2022-0152**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0152.json	A-GIT-GITL-030222/30
Cross-Site Request Forgery (CSRF)	18-Jan-22	6	An issue has been discovered in GitLab affecting all versions starting from 7.7 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to a Cross-Site Request Forgery attack that allows a malicious user to have their GitHub project imported on another	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0154.json	A-GIT-GITL-030222/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GitLab user account. **CVE ID : CVE-2022-0154**		
Incorrect Authorization	18-Jan-22	6.4	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.3. Under certain conditions it was possible to bypass the IP restriction for public projects through GraphQL allowing unauthorised users to read titles of issues, merge requests and milestones. **CVE ID : CVE-2022-0172**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0172.json	A-GIT-GITL-030222/32
Files or Directories Accessible to External Parties	18-Jan-22	5	An issue has been discovered in GitLab CE/EE affecting all versions starting with 14.5. Arbitrary file read was possible by importing a group was due to incorrect handling of file. **CVE ID : CVE-2022-0244**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-0244.json, https://gitlab.com/gitlab-org/gitlab/-/issues/349524	A-GIT-GITL-030222/33
grafana					
grafana					
Exposure of Sensitive Information to an Unauthorized Actor	18-Jan-22	3.5	Grafana is an open-source platform for monitoring and observability. In affected versions when a data source has the Forward OAuth Identity feature enabled, sending a query to that datasource with an API token (and no other user credentials) will forward the OAuth Identity of the most recently logged-in user. This	https://github.com/grafana/grafana/security/advisories/GHSA-8wjh-59cw-9xh4	A-GRA-GRAF-030222/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can allow API token holders to retrieve data for which they may not have intended access. This attack relies on the Grafana instance having data sources that support the Forward OAuth Identity feature, the Grafana instance having a data source with the Forward OAuth Identity feature toggled on, the Grafana instance having OAuth enabled, and the Grafana instance having usable API keys. This issue has been patched in versions 7.5.13 and 8.3.4. **CVE ID : CVE-2022-21673**		
graphql-go_project					
graphql-go					
Uncontrolled Resource Consumption	21-Jan-22	3.5	graphql-go is a GraphQL server with a focus on ease of use. In versions prior to 1.3.0 there exists a DoS vulnerability that is possible due to a bug in the library that would allow an attacker with specifically designed queries to cause stack overflow panics. Any user with access to the GraphQL handler can send these queries and cause stack overflows. This in turn could potentially compromise the ability of the server to serve data to its users. The issue has been patched in version `v1.3.0`. The only known workaround for this issue is	https://github.com/graph-gophers/graphql-go/security/advisories/GHSA-mh3m-8c74-74xh, https://github.com/graph-gophers/graphql-go/commit/eae31ca73eb3473c544710955d1dbebc22605bfe	A-GRA-GRAP-030222/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to disable the `graphql.MaxDepth` option from your schema which is not recommended. **CVE ID : CVE-2022-21708**		
h2database					
h2					
Improper Control of Generation of Code ('Code Injection')	19-Jan-22	10	H2 Console before 2.1.210 allows remote attackers to execute arbitrary code via a jdbc:h2:mem JDBC URL containing the IGNORE_UNKNOWN_SETTINGS=TRUE;FORBID_CREATION=FALSE;INIT=RUNSCRIPT substring, a different vulnerability than CVE-2021-42392. **CVE ID : CVE-2022-23221**	https://github.com/h2database/h2database/security/advisories , https://github.com/h2database/h2database/releases/tag/version-2.1.210	A-H2D-H2-030222/36
hms_project					
hms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jan-22	7.5	HMS v1.0 was discovered to contain a SQL injection vulnerability via adminlogin.php. **CVE ID : CVE-2022-23364**	N/A	A-HMS-HMS-030222/37
Improper Neutralization of Special Elements used in an SQL Command ('SQL	21-Jan-22	7.5	HMS v1.0 was discovered to contain a SQL injection vulnerability via doctorlogin.php. **CVE ID : CVE-2022-23365**	N/A	A-HMS-HMS-030222/38

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jan-22	7.5	HMS v1.0 was discovered to contain a SQL injection vulnerability via patientlogin.php. **CVE ID : CVE-2022-23366**	N/A	A-HMS-HMS-030222/39
hospital\\'s_patient_records_management_system_project					
hospital\\'s_patient_records_management_system					
Incorrect Default Permissions	24-Jan-22	5	Sourcecodester Hospital's Patient Records Management System 1.0 is vulnerable to Insecure Permissions via the id parameter in manage_user endpoint. Simply change the value and data of other users can be displayed. **CVE ID : CVE-2022-22296**	N/A	A-HOS-HOSP-030222/40
IBM					
websphere_application_server					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	A-IBM-WEBS-030222/41
Iconics					
analytix					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Jan-22	7.5	Incomplete List of Disallowed Inputs vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.95.3 to 10.97, ICONICS Hyper Historian versions 10.95.3 to 10.97, ICONICS AnalytiX versions 10.95.3 to 10.97 and ICONICS MobileHMI versions 10.95.3 to 10.97 allows a remote unauthenticated attacker to bypass the authentication of MC Works64, GENESIS64, Hyper Historian, AnalytiX and MobileHMI, and gain unauthorized access to the products, by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of the products. **CVE ID : CVE-2022-23128**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-026_en.pdf	A-ICO-ANAL-030222/42
genesis64					
N/A	21-Jan-22	7.5	Incomplete List of Disallowed Inputs vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.95.3 to 10.97, ICONICS Hyper Historian versions 10.95.3 to 10.97, ICONICS AnalytiX versions 10.95.3 to 10.97 and ICONICS MobileHMI versions 10.95.3 to 10.97 allows a	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-026_en.pdf	A-ICO-GENE-030222/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to bypass the authentication of MC Works64, GENESIS64, Hyper Historian, AnalytiX and MobileHMI, and gain unauthorized access to the products, by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of the products. **CVE ID : CVE-2022-23128**		
Cleartext Storage of Sensitive Information	21-Jan-22	2.1	Plaintext Storage of a Password vulnerability in Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior and ICONICS GENESIS64 versions 10.90 to 10.97 allows a local authenticated attacker to gain authentication information and to access the database illegally. This is because when configuration information of GridWorX, a database linkage function of GENESIS64 and MC Works64, is exported to a CSV file, the authentication information is saved in plaintext, and an attacker who can access this CSV file can gain the authentication information. **CVE ID : CVE-2022-23129**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-027_en.pdf	A-ICO-GENE-030222/44
Out-of-bounds Read	21-Jan-22	4.3	Buffer Over-read vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E	https://www.mitsubishielectric.com/en/psirt/vulnerability/pd	A-ICO-GENE-030222/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(10.95.210.01), ICONICS GENESIS64 versions 10.97 and prior and ICONICS Hyper Historian versions 10.97 and prior allows an attacker to cause a DoS condition in the database server by getting a legitimate user to import a configuration file containing specially crafted stored procedures into GENESIS64 or MC Works64 and execute commands against the database from GENESIS64 or MC Works64. **CVE ID : CVE-2022-23130**	f/2021-028_en.pdf	
hyper_historian					
N/A	21-Jan-22	7.5	Incomplete List of Disallowed Inputs vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.95.3 to 10.97, ICONICS Hyper Historian versions 10.95.3 to 10.97, ICONICS AnalytiX versions 10.95.3 to 10.97 and ICONICS MobileHMI versions 10.95.3 to 10.97 allows a remote unauthenticated attacker to bypass the authentication of MC Works64, GENESIS64, Hyper Historian, AnalytiX and MobileHMI, and gain unauthorized access to the products, by sending specially crafted WebSocket packets to FrameWorX	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-026_en.pdf	A-ICO-HYPE-030222/46

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server, one of the functions of the products. **CVE ID : CVE-2022-23128**		
Out-of-bounds Read	21-Jan-22	4.3	Buffer Over-read vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.97 and prior and ICONICS Hyper Historian versions 10.97 and prior allows an attacker to cause a DoS condition in the database server by getting a legitimate user to import a configuration file containing specially crafted stored procedures into GENESIS64 or MC Works64 and execute commands against the database from GENESIS64 or MC Works64. **CVE ID : CVE-2022-23130**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-028_en.pdf	A-ICO-HYPE-030222/47
mobilehmi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jan-22	4.3	Cross-site Scripting vulnerability in Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior and ICONICS MobileHMI versions 10.96.2 and prior allows a remote unauthenticated attacker to gain authentication information of an MC Works64 or MobileHMI and perform any operation using the acquired authentication information,	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-025_en.pdf	A-ICO-MOBI-030222/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by injecting a malicious script in the URL of a monitoring screen delivered from the MC Works64 server or MobileHMI server to an application for mobile devices and leading a legitimate user to access this URL. **CVE ID : CVE-2022-23127**		
N/A	21-Jan-22	7.5	Incomplete List of Disallowed Inputs vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.95.3 to 10.97, ICONICS Hyper Historian versions 10.95.3 to 10.97, ICONICS AnalytiX versions 10.95.3 to 10.97 and ICONICS MobileHMI versions 10.95.3 to 10.97 allows a remote unauthenticated attacker to bypass the authentication of MC Works64, GENESIS64, Hyper Historian, AnalytiX and MobileHMI, and gain unauthorized access to the products, by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of the products. **CVE ID : CVE-2022-23128**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-026_en.pdf	A-ICO-MOBI-030222/49
Ipython					
ipython					
Improper	19-Jan-22	4.6	IPython (Interactive Python)	https://githu	A-IPY-IPYT-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			is a command shell for interactive computing in multiple programming languages, originally developed for the Python programming language. Affected versions are subject to an arbitrary code execution vulnerability achieved by not properly managing cross user temporary files. This vulnerability allows one user to run code as another on the same machine. All users are advised to upgrade. **CVE ID : CVE-2022-21699**	b.com/ipython/ipython/security/advisories/GHSA-pq7m-3gw7-gq5x, https://github.com/ipython/ipython/commit/46a51ed69cdf41b4333943d9ceeb945c4ede5668	030222/50
istio					
istio					
Always-Incorrect Control Flow Implementation	19-Jan-22	7.5	Istio is an open platform to connect, manage, and secure microservices. In Istio 1.12.0 and 1.12.1 The authorization policy with hosts and notHosts might be accidentally bypassed for ALLOW action or rejected unexpectedly for DENY action during the upgrade from 1.11 to 1.12.0/1.12.1. Istio 1.12 supports the hosts and notHosts fields in authorization policy with a new Envoy API shipped with the 1.12 data plane. A bug in the 1.12.0 and 1.12.1 incorrectly uses the new Envoy API with the 1.11 data plane. This will cause the hosts and notHosts fields to	https://istio.io/latest/news/releases/1.12.x/announcing-1.12.2/, https://github.com/istio/istio/security/advisories/GHSA-rwfr-xrvw-2rvv	A-IST-ISTI-030222/51

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be always matched regardless of the actual value of the host header when mixing 1.12.0/1.12.1 control plane and 1.11 data plane. Users are advised to upgrade or to not mix the 1.12.0/1.12.1 control plane with 1.11 data plane if using hosts or notHosts field in authorization policy. **CVE ID : CVE-2022-21679**		
Incorrect Authorization	19-Jan-22	6	Istio is an open platform to connect, manage, and secure microservices. In versions 1.12.0 and 1.12.1 Istio is vulnerable to a privilege escalation attack. Users who have `CREATE` permission for `gateways.gateway.networking.k8s.io` objects can escalate this privilege to create other resources that they may not have access to, such as `Pod`. This vulnerability impacts only an Alpha level feature, the Kubernetes Gateway API. This is not the same as the Istio Gateway type (gateways.networking.istio.io), which is not vulnerable. Users are advised to upgrade to resolve this issue. Users unable to upgrade should implement any of the following which will prevent this vulnerability: Remove the gateways.gateway.networkin	https://istio.io/latest/news/releases/1.12.x/announcing-1.12.2/, https://github.com/istio/istio/security/advisories/GHSA-mq8f-9446-c28r	A-IST-ISTI-030222/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			g.k8s.io CustomResourceDefinition, set PILOT_ENABLE_GATEWAY_API_DEPLOYMENT_CONTROLLER=true environment variable in Istiod, or remove CREATE permissions for gateways.gateway.networking.k8s.io objects from untrusted users. **CVE ID : CVE-2022-21701**		
jadx_project					
jadx					
Improper Restriction of XML External Entity Reference	20-Jan-22	4.3	Improper Restriction of XML External Entity Reference in GitHub repository skylot/jadx prior to 1.3.2. **CVE ID : CVE-2022-0219**	https://huntr.dev/bounties/0d093863-29e8-4dd7-a885-64f76d50bf5e, https://github.com/skylot/jadx/commit/d22db30166e7cb369d72be41382bb63ac8b81c52	A-JAD-JADX-030222/53
Jerryscript					
jerryscript					
Out-of-bounds Write	20-Jan-22	6.8	Jerryscript 3.0.0 was discovered to contain a stack overflow via ecma_op_object_find_own in /ecma/operations/ecma-objects.c. **CVE ID : CVE-2022-22888**	https://github.com/jerryscript-project/jerryscript/issues/4848	A-JER-JERR-030222/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	20-Jan-22	5	There is an Assertion 'arguments_type != SCANNER_ARGUMENTS_PRESENT && arguments_type != SCANNER_ARGUMENTS_PRESENT_NO_REG' failed at /jerry-core/parser/js/js-scanner-util.c in Jerryscript 3.0.0. **CVE ID : CVE-2022-22890**	https://github.com/jerryscript-project/jerryscript/issues/4847	A-JER-JERR-030222/55
N/A	21-Jan-22	4.3	Jerryscript 3.0.0 was discovered to contain a SEGV vulnerability via ecma_ref_object_inline in /jerry-core/ecma/base/ecma-gc.c. **CVE ID : CVE-2022-22891**	https://github.com/jerryscript-project/jerryscript/issues/4871	A-JER-JERR-030222/56
Reachable Assertion	21-Jan-22	4.3	There is an Assertion 'ecma_is_value_undefined (value) || ecma_is_value_null (value) || ecma_is_value_boolean (value) || ecma_is_value_number (value) || ecma_is_value_string (value) || ecma_is_value_bigint (value) || ecma_is_value_symbol (value) || ecma_is_value_object (value)' failed at jerry-core/ecma/base/ecma-helpers-value.c in Jerryscripts 3.0.0. **CVE ID : CVE-2022-22892**	https://github.com/jerryscript-project/jerryscript/issues/4872	A-JER-JERR-030222/57
Out-of-bounds Write	21-Jan-22	6.8	Jerryscript 3.0.0 was discovered to contain a stack overflow via vm_loop.lto_priv.304 in	https://github.com/jerryscript-project/jerry	A-JER-JERR-030222/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/jerry-core/vm/vm.c. **CVE ID : CVE-2022-22893**	script/issues/4901	
Out-of-bounds Write	21-Jan-22	6.8	Jerryscript 3.0.0 was discovered to contain a stack overflow via ecma_lcache_lookup in /jerry-core/ecma/base/ecma-lcache.c. **CVE ID : CVE-2022-22894**	https://github.com/jerryscript-project/jerryscript/issues/4890	A-JER-JERR-030222/59
Out-of-bounds Write	21-Jan-22	6.8	Jerryscript 3.0.0 was discovered to contain a heap-buffer-overflow via ecma_utf8_string_to_number_by_radix in /jerry-core/ecma/base/ecma-helpers-conversion.c. **CVE ID : CVE-2022-22895**	https://github.com/jerryscript-project/jerryscript/issues/4850, https://github.com/jerryscript-project/jerryscript/issues/4882	A-JER-JERR-030222/60
jmty					
jimoty					
Use of Hard-coded Credentials	17-Jan-22	2.1	Jimoty App for Android versions prior to 3.7.42 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app. **CVE ID : CVE-2022-0131**	N/A	A-JMT-JIMO-030222/61
Juniper					
contrail_service_orchestration					
Protection Mechanism	19-Jan-22	4	A Protection Mechanism Failure vulnerability in the	https://kb.juniper.net/JS	A-JUN-CONT-030222/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Failure			REST API of Juniper Networks Contrail Service Orchestration allows one tenant on the system to view confidential configuration details of another tenant on the same system. By utilizing the REST API, one tenant is able to obtain information on another tenant's firewall configuration and access control policies, as well as other sensitive information, exposing the tenant to reduced defense against malicious attacks or exploitation via additional undetermined vulnerabilities. This issue affects Juniper Networks Contrail Service Orchestration versions prior to 6.1.0 Patch 3. **CVE ID : CVE-2022-22152**	A11260	
kingjim					
sma3					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	https://www.kingjim.co.jp/download/security/#sr01	A-KIN-SMA3-030222/63
libexpat_project					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libexpat					
Integer Overflow or Wraparound	24-Jan-22	7.5	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES. **CVE ID : CVE-2022-23852**	https://github.com/libexpat/libexpat/pull/550	A-LIB-LIBE-030222/64
Integer Overflow or Wraparound	26-Jan-22	7.5	Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function. **CVE ID : CVE-2022-23990**	https://github.com/libexpat/libexpat/pull/551	A-LIB-LIBE-030222/65
Linecorp					
line					
Uncontrolled Resource Consumption	20-Jan-22	4.3	Due to the lack of media file checks before rendering, it was possible for an attacker to cause abnormal CPU consumption for message recipient by sending specially crafted gif image in LINE for Windows before 7.4. **CVE ID : CVE-2022-22820**	N/A	A-LIN-LINE-030222/66
livehelperchat					
livehelperchat					
Cross-Site Request Forgery (CSRF)	18-Jan-22	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository livehelperchat/livehelperchat prior to 2.0. **CVE ID : CVE-2022-0245**	https://huntr.dev/bounties/6a6aca72-32b7-45b3-a8ba-9b400b2d669c, https://github.com/livehelperchat/livehelperchat/commit/c2fa1	A-LIV-LIVE-030222/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9afeb8b1ea927fea3fd452515c95f289fb9	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-22	3.5	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2022-0253**	https://github.com/livehelperchat/livehelperchat/commit/407d0b1a1fa56fa6f824a19092774f10f4880437, https://huntr.dev/bounties/ac7f7eba-ee0b-4a50-bd89-29fd9b3e8303	A-LIV-LIVE-030222/68
live_helper_chat					
Authorization Bypass Through User-Controlled Key	19-Jan-22	6	Authorization Bypass Through User-Controlled Key in Packagist remdex/livehelperchat prior to 3.92v. **CVE ID : CVE-2022-0266**	https://github.com/livehelperchat/livehelperchat/commit/cc1122aed0d1ad9f05757eaea2ab9e6a924776bd, https://huntr.dev/bounties/1ac267be-3af8-4774-89f2-77234d144d6b	A-LIV-LIVE-030222/69
log4js_project					
log4js					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	19-Jan-22	2.1	log4js-node is a port of log4js to node.js. In affected versions default file permissions for log files created by the file, fileSync and dateFile appenders are world-readable (in unix). This could cause problems if log files contain sensitive information. This would affect any users that have not supplied their own permissions for the files via the mode parameter in the config. Users are advised to update. **CVE ID : CVE-2022-21704**	https://github.com/log4js-node/log4js-node/pull/1141/commits/8042252861a1b65adb66931fdf702ead34fa9b76, https://github.com/log4js-node/streamroller/pull/87, https://github.com/log4js-node/log4js-node/security/advisories/GHSA-82v2-mx6x-wq7q	A-LOG-LOG4-030222/70
loguru_project					
loguru					
Improper Control of Generation of Code ('Code Injection')	21-Jan-22	7.5	Code Injection in PyPi loguru prior to and including 0.5.3. **CVE ID : CVE-2022-0329**	https://github.com/delgan/loguru/commit/4b0070a4f30cbf6d5e12e6274b242b62ea11c81b, https://huntr.dev/bounties/1-pypi-loguru	A-LOG-LOGU-030222/71

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Mcafee					
agent					
Improper Privilege Management	19-Jan-22	7.2	A privilege escalation vulnerability in the McAfee Agent prior to 5.7.5. McAfee Agent uses openssl.cnf during the build process to specify the OPENSSLDIR variable as a subdirectory within the installation directory. A low privilege user could have created subdirectories and executed arbitrary code with SYSTEM privileges by creating the appropriate pathway to the specifically created malicious openssl.cnf file. **CVE ID : CVE-2022-0166**	https://kc.mcafee.com/corporate/index?page=content&id=SB10378	A-MCA-AGEN-030222/72
Mediawiki					
shortdescription					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-22	4.3	ShortDescription is a MediaWiki extension that provides local short description support. A cross-site scripting (XSS) vulnerability exists in versions prior to 2.3.4. On a wiki that has the ShortDescription enabled, XSS can be triggered on any page or the page with the action=info parameter, which displays the shortdesc property. This is achieved using the wikitext `{{SHORTDESC:&lt;img src=x onerror=alert()&gt;}}`. This issue has a patch in version	https://github.com/StarCitizenTools/mediawiki-extensions-ShortDescription/commit/bf568edd892adb8528dcb64f75dddf3eeaccc12c, https://github.com/StarCitizenTools/mediawiki-extensions-ShortDescription/commit	A-MED-SHOR-030222/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.4. **CVE ID : CVE-2022-21710**	/7c86644158388620c6c858258cc4e1a8de6e48ea	
metagauss					
leadmagic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	3.5	The User Registration, Login & Landing Pages WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the loader_text parameter found in the ~/includes/templates/landing-page.php file which allows attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.2.7. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled. **CVE ID : CVE-2022-0232**	N/A	A-MET-LEAD-030222/74
profilegrid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	3.5	The ProfileGrid – User Profiles, Memberships, Groups and Communities WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the pm_user_avatar and pm_cover_image parameters found in the ~/admin/class-profile-magic-admin.php file which allows attackers with authenticated user access,	N/A	A-MET-PROF-030222/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			such as subscribers, to inject arbitrary web scripts into their profile, in versions up to and including 1.2.7. **CVE ID : CVE-2022-0233**		
Microweber					
microweber					
Improper Privilege Management	20-Jan-22	4	Improper Access Control in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0277**	https://github.com/microweber/microweber/commit/e680e134a4215c979bfd2eaf58336be34c8fc6e6, https://huntr.dev/bounties/0e776f3d-35b1-4a9e-8fe8-91e46c0d6316	A-MIC-MICR-030222/76
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0278**	https://github.com/microweber/microweber/commit/b64ef574b82dbf89a908e1569d790c7012d1ccd7, https://huntr.dev/bounties/64495d0f-d5ec-4542-9693-32372c18d030	A-MIC-MICR-030222/77

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	20-Jan-22	5	Exposure of Sensitive Information to an Unauthorized Actor in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0281**	https://github.com/microweber/microweber/commit/e680e134a4215c979bfd2eaf58336be34c8fc6e6, https://huntr.dev/bounties/315f5ac6-1b5e-4444-ad8f-802371da3505	A-MIC-MICR-030222/78
Improper Control of Generation of Code ('Code Injection')	20-Jan-22	5	Code Injection in Packagist microweber/microweber prior to 1.2.11. **CVE ID : CVE-2022-0282**	https://github.com/microweber/microweber/commit/51b5a4e3ef01e587797c0109159a8ad9d2bac77a, https://huntr.dev/bounties/8815b642-bd9b-4737-951b-bde7319faedd	A-MIC-MICR-030222/79
mingsoft					
mcms					
Use of Hard-coded Credentials	21-Jan-22	7.5	MCMS v5.2.4 was discovered to have a hardcoded shiro-key, allowing attackers to exploit the key and execute arbitrary code.	N/A	A-MIN-MCMS-030222/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22928		
Unrestricted Upload of File with Dangerous Type	21-Jan-22	7.5	MCMS v5.2.4 was discovered to have an arbitrary file upload vulnerability in the New Template module, which allows attackers to execute arbitrary code via a crafted ZIP file. **CVE ID : CVE-2022-22929**	N/A	A-MIN-MCMS-030222/81
N/A	21-Jan-22	7.5	A remote code execution (RCE) vulnerability in the Template Management function of MCMS v5.2.4 allows attackers to execute arbitrary code via a crafted payload. **CVE ID : CVE-2022-22930**	N/A	A-MIN-MCMS-030222/82
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jan-22	7.5	MCMS v5.2.4 was discovered to contain a SQL injection vulnerability via /ms/mdiy/model/importJson.do. **CVE ID : CVE-2022-23314**	N/A	A-MIN-MCMS-030222/83
Unrestricted Upload of File with Dangerous Type	21-Jan-22	7.5	MCMS v5.2.4 was discovered to contain an arbitrary file upload vulnerability via the component /ms/template/writeFileContent.do. **CVE ID : CVE-2022-23315**	N/A	A-MIN-MCMS-030222/84
Mitsubishielectric					
mc_works64					
Improper Neutralization of Input	21-Jan-22	4.3	Cross-site Scripting vulnerability in Mitsubishi Electric MC Works64	https://www.mitsubishielectric.com/	A-MIT-MC_W-030222/85

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			versions 4.04E (10.95.210.01) and prior and ICONICS MobileHMI versions 10.96.2 and prior allows a remote unauthenticated attacker to gain authentication information of an MC Works64 or MobileHMI and perform any operation using the acquired authentication information, by injecting a malicious script in the URL of a monitoring screen delivered from the MC Works64 server or MobileHMI server to an application for mobile devices and leading a legitimate user to access this URL. **CVE ID : CVE-2022-23127**	en/psirt/vulnerability/pdf/2021-025_en.pdf	
N/A	21-Jan-22	7.5	Incomplete List of Disallowed Inputs vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.95.3 to 10.97, ICONICS Hyper Historian versions 10.95.3 to 10.97, ICONICS AnalytiX versions 10.95.3 to 10.97 and ICONICS MobileHMI versions 10.95.3 to 10.97 allows a remote unauthenticated attacker to bypass the authentication of MC Works64, GENESIS64, Hyper Historian, AnalytiX and MobileHMI, and gain	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-026_en.pdf	A-MIT-MC_W-030222/86

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to the products, by sending specially crafted WebSocket packets to FrameWorX server, one of the functions of the products. **CVE ID : CVE-2022-23128**		
Cleartext Storage of Sensitive Information	21-Jan-22	2.1	Plaintext Storage of a Password vulnerability in Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior and ICONICS GENESIS64 versions 10.90 to 10.97 allows a local authenticated attacker to gain authentication information and to access the database illegally. This is because when configuration information of GridWorX, a database linkage function of GENESIS64 and MC Works64, is exported to a CSV file, the authentication information is saved in plaintext, and an attacker who can access this CSV file can gain the authentication information. **CVE ID : CVE-2022-23129**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-027_en.pdf	A-MIT-MC_W-030222/87
Out-of-bounds Read	21-Jan-22	4.3	Buffer Over-read vulnerability in Mitsubishi Electric MC Works64 versions 4.00A (10.95.201.23) to 4.04E (10.95.210.01), ICONICS GENESIS64 versions 10.97 and prior and ICONICS Hyper Historian versions 10.97 and prior allows an attacker to cause a DoS condition in the	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-028_en.pdf	A-MIT-MC_W-030222/88

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			database server by getting a legitimate user to import a configuration file containing specially crafted stored procedures into GENESIS64 or MC Works64 and execute commands against the database from GENESIS64 or MC Works64. **CVE ID : CVE-2022-23130**		
mruby					
mruby					
NULL Pointer Dereference	17-Jan-22	5	mruby is vulnerable to NULL Pointer Dereference **CVE ID : CVE-2022-0240**	https://huntr.dev/bounties/5857eced-aad9-417d-864e-0bdf17226cbb, https://github.com/mruby/mruby/commit/31fa3304049fc406a201a72293cce140f0557dca	A-MRU-MRUB-030222/89
NULL Pointer Dereference	21-Jan-22	4.3	NULL Pointer Dereference in Homebrew mruby prior to 3.2. **CVE ID : CVE-2022-0326**	https://huntr.dev/bounties/795dcbd9-1695-44bb-8c59-ad327c97c976, https://github.com/mruby/mruby/commit/b611c43a5de061e	A-MRU-MRUB-030222/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				c21b343967e1b64c45c373d7e	
mustache_project					
mustache					
N/A	21-Jan-22	6.5	Improper Neutralization of Special Elements Used in a Template Engine in Packagist mustache/mustache prior to 2.14.1. **CVE ID : CVE-2022-0323**	https://github.com/bobthecow/mustache.php/commit/579ffa5c96e1d292c060b3dd62811ff01ad8c24e, https://huntr.dev/bounties/a5f5a988-aa52-4443-839d-299a63f44fb7	A-MUS-MUST-030222/91
navidrome					
navidrome					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jan-22	4	model/criteria/criteria.go in Navidrome before 0.47.5 is vulnerable to SQL injection attacks when processing crafted Smart Playlists. An authenticated user could abuse this to extract arbitrary data from the database, including the user table (which contains sensitive information such as the users' encrypted passwords). **CVE ID : CVE-2022-23857**	https://github.com/navidrome/navidrome/commit/9e79b5cbf2a48c1e4344df00fea4ed3844ea965d	A-NAV-NAVI-030222/92
Netapp					
cloud_insights					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g.,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/98

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/102

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-CLOU-030222/104

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-CLOU-030222/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**	om/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuja	A-NET-CLOU-030222/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com	A-NET-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	030222/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-CLOU-030222/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
e-series_santricity_os_controller					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/111

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/117

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-	A-NET-E-SE-030222/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**	20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-E-SE-030222/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**	rity.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-NET-E-SE-030222/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟨	Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**	alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
e-series_santricity_storage_manager					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/127

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-	A-NET-E-SE-030222/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**	20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-E-SE-030222/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**	rity.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-NET-E-SE-030222/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**	alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle	https://ww	A-NET-E-SE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	030222/136

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21299		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/140

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/141

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
e-series_santricity_web_services					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-E-SE-030222/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-NET-E-SE-030222/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**	/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-E-SE-030222/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**	https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com	A-NET-E-SE-030222/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/158

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-E-SE-030222/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
oncommand_insight					
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21245**		
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21249**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/163
N/A	19-Jan-22	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported	https://www.oracle.com/security-alerts/cpuja	A-NET-ONCO-030222/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21253**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit 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 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).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21254		
N/A	19-Jan-22	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21256**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/166
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21264**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21265**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/168
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-ONCO-030222/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21270**	om/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/170

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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 as well as unauthorized update,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21278**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21279**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/173
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle	https://www.oracle.com	A-NET-ONCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21280**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/174
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/176

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-NET-ONCO-030222/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21284**	/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21285**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21286**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/179
N/A	19-Jan-22	4	Vulnerability in the MySQL	https://ww	A-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21287**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	ONCO-030222/180
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21288**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/182

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21289**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21290**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/183
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-ONCO-030222/184

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**	om/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuja	A-NET-ONCO-030222/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle	https://ww	A-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	ONCO-030222/186

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21294		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/187

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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). **CVE ID : CVE-2022-21297**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/188
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/190

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21301**		
N/A	19-Jan-22	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit 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 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). **CVE ID : CVE-2022-21302**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/191
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported	https://www.oracle.com/security-alerts/cpuja	A-NET-ONCO-030222/192

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21303**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21304**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21307**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/195
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-ONCO-030222/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21308**	rity.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/197

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21309**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21310**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/198
N/A	19-Jan-22	2.9	Vulnerability in the MySQL	https://ww	A-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21311**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	ONCO-030222/199
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-ONCO-030222/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21312**	om/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21313**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21314**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21315**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/203
N/A	19-Jan-22	4.6	Vulnerability in the MySQL Cluster product of Oracle	https://www.oracle.com	A-NET-ONCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21316**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/204
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21317**		
N/A	19-Jan-22	4.6	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21318**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21319**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/207
N/A	19-Jan-22	4	Vulnerability in the MySQL	https://ww	A-NET-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21320**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	ONCO-030222/208
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/209

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21321**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/210

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21322**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21323**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21324**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/212
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior,	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-ONCO-030222/213

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21325**	rity.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/214

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21326**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21327**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21328**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/216
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-ONCO-030222/217

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21329**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/218

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21330**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21331**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21332**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/220
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-ONCO-030222/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21333**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/222

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21334**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21335**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21336**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/224
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior,	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-ONCO-030222/225

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21337**	rity.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21339**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21342**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/229
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-ONCO-030222/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21344**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21348**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/231

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21349		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21351**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/233
N/A	19-Jan-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.26 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2022-21352**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/235

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21355**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21356**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/236
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle	https://www.oracle.com	A-NET-ONCO-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21357**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/237
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-NET-ONCO-030222/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21358**	/ntap-20220121-0008/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/240

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21362		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/241

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-ONCO-030222/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21367**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/243
N/A	19-Jan-22	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.27 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-ONCO-030222/244

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 as well as unauthorized read access to a subset 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 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2022-21368**	om/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21370**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21372**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/246
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21374**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21378**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/248
N/A	19-Jan-22	4	Vulnerability in the MySQL	https://ww	A-NET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21379**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	ONCO-030222/249
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/250

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21380**		
oncommand_workflow_automation					
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21245**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/251
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions	https://www.oracle.com/security-alerts/cpuja	A-NET-ONCO-030222/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21249**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/253

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21253		
N/A	19-Jan-22	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit 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 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). **CVE ID : CVE-2022-21254**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/254
N/A	19-Jan-22	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21256**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21264**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/256
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/257

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21265**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21270**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/258
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle	https://www.oracle.com	A-NET-ONCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21278**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/259
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21279**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21280**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21284**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/262
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-NET-ONCO-030222/263

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21285**	/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21286**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21287**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/265
N/A	19-Jan-22	4	Vulnerability in the MySQL	https://ww	A-NET-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21288**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	ONCO-030222/266
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21289**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/268

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21290**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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). **CVE ID : CVE-2022-21297**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/269
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/270

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21301**		
N/A	19-Jan-22	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit 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 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). **CVE ID : CVE-2022-21302**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/271
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-ONCO-030222/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21303**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21304		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21307**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/274
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-ONCO-030222/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21308**	0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21309**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21310**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/277
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-ONCO-030222/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21311**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/279

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21312**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21313**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21314**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21315**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/282
N/A	19-Jan-22	4.6	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior,	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-ONCO-030222/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21316**	rity.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21317**		
N/A	19-Jan-22	4.6	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21318		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21319**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/286
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-ONCO-030222/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21320**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/288

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21321**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21322**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21323**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/290
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions	https://www.oracle.com/security-alerts/cpuja	A-NET-ONCO-030222/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21324**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-ONCO-030222/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21325**	0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21326**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21327**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21328**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/295
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-	A-NET-ONCO-030222/296

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21329**	20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/297

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21330**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21331**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21332**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/299
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-	A-NET-ONCO-030222/300

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21333**	20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21334**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21335		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21336**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/303
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-ONCO-030222/304

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21337**	0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/305

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21339**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21342**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/306
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21344**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21348**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/308
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-ONCO-030222/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21351**	0008/	
N/A	19-Jan-22	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2022-21352**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21355**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/311
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle	https://www.oracle.com	A-NET-ONCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21356**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/312
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/313

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21357**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 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).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/314

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21358**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21362**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/315
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21367**		
N/A	19-Jan-22	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.27 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 as well as unauthorized read access to a subset 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 4.7 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2022-21368**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21370**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/318
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21372**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21374**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/320
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-ONCO-030222/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21378**	om/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/322

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21379**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21380**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-ONCO-030222/323
santricity_unified_manager					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-NET-SANT-030222/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**	rity.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-NET-SANT-030222/325

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**	alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/326

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/330

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/335

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SANT-030222/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-SANT-030222/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-NET-SANT-030222/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**	/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-SANT-030222/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**	https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com	A-NET-SANT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	030222/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
snapcenter					
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21322**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-NET-SNAP-030222/341
snapmanager					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-SNAP-030222/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-NET-SNAP-030222/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**	/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions	https://www.oracle.com/security-alerts/cpujan2022.html,	A-NET-SNAP-030222/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**	https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com	A-NET-SNAP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	030222/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/346

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g.,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/354

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-NET-SNAP-030222/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-NET-SNAP-030222/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01;	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-NET-SNAP-030222/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**	om/advisory/ntap-20220121-0007/	
node-fetch_project					
node-fetch					
URL Redirection	16-Jan-22	5.8	node-fetch is vulnerable to Exposure of Sensitive	https://huntr.dev/bounti	A-NOD-NODE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to Untrusted Site ('Open Redirect')			Information to an Unauthorized Actor **CVE ID : CVE-2022-0235**	es/d26ab655-38d6-48b3-be15-f9ad6b6ae6f7, https://github.com/node-fetch/node-fetch/commit/36e47e8a6406185921e4985dcbeff140d73eaa10	030222/359
objectcomputing					
micronaut					
Uncontrolled Resource Consumption	18-Jan-22	5	Micronaut is a JVM-based, full stack Java framework designed for building JVM web applications with support for Java, Kotlin and the Groovy language. In affected versions sending an invalid Content Type header leads to memory leak in DefaultArgumentConversionContext as this type is erroneously used in static state. ### Impact Sending an invalid Content Type header leads to memory leak in `DefaultArgumentConversionContext` as this type is erroneously used in static state. ### Patches The problem is patched in Micronaut 3.2.7 and above. ### Workarounds The default content type binder can be replaced in an existing Micronaut application to	https://github.com/micronaut-projects/micronaut-core/commit/b8ec32c311689667c69ae7d9f9c3b3a8abc96fe3, https://github.com/micronaut-projects/micronaut-core/security/advisories/GHSA-2457-2263-mm9f	A-OBJ-MICR-030222/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigate the issue: ```java package example; import java.util.List; import io.micronaut.context.annotation.Replaces; import io.micronaut.core.convert.ConversionService; import io.micronaut.http.MediaType; import io.micronaut.http.bind.DefaultRequestBinderRegistry; import io.micronaut.http.bind.binders.RequestArgumentBinder; import jakarta.inject.Singleton; @Singleton @Replaces(DefaultRequestBinderRegistry.class) class FixedRequestBinderRegistry extends DefaultRequestBinderRegistry { public FixedRequestBinderRegistry(ConversionService conversionService, List<RequestArgumentBinder> binders) { super(conversionService, binders); } @Override protected void registerDefaultConverters(ConversionService<?> conversionService) { super.registerDefaultConverters(conversionService); conversionService.addConverter(CharSequence.class, MediaType.class, charSequence -> { try { return MediaType.of(charSequence);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			} catch (IllegalArgumentException e) { return null; } }); } } ``` ### References Commit that introduced the vulnerability https://github.com/micronaut-projects/micronaut-core/commit/b8ec32c311689667c69ae7d9f9c3b3a8abc96fe3 ### For more information If you have any questions or comments about this advisory: * Open an issue in [Micronaut Core](https://github.com/micronaut-projects/micronaut-core/issues) * Email us at info@micronaut.io **CVE ID : CVE-2022-21700**		
Onionshare					
onionshare					
Out-of-bounds Read	18-Jan-22	4.3	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. Affected versions of the desktop application were found to be vulnerable to denial of service via an undisclosed vulnerability in the QT image parsing. Roughly 20 bytes lead to 2GB memory consumption and this can be triggered multiple times. To be abused, this vulnerability requires rendering in the history tab, so some user interaction is	https://github.com/onionshare/onionshare/security/advisories/GHSA-x7wr-283h-5h2v	A-ONI-ONIO-030222/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required. An adversary with knowledge of the Onion service address in public mode or with authentication in private mode can perform a Denial of Service attack, which quickly results in out-of-memory for the server. This requires the desktop application with rendered history, therefore the impact is only elevated. This issue has been patched in version 2.5. **CVE ID : CVE-2022-21688**		
Uncontrolled Resource Consumption	18-Jan-22	5	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions the receive mode limits concurrent uploads to 100 per second and blocks other uploads in the same second, which can be triggered by a simple script. An adversary with access to the receive mode can block file upload for others. There is no way to block this attack in public mode due to the anonymity properties of the tor network. **CVE ID : CVE-2022-21689**	https://github.com/onionshare/onionshare/security/advisories/GHSA-jh82-c5jw-pxpc	A-ONI-ONIO-030222/362
Improper Neutralization of Input During Web Page Generation	18-Jan-22	3.5	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions	https://github.com/onionshare/onionshare/security/advisories/GHSA-ch22-	A-ONI-ONIO-030222/363

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			The path parameter of the requested URL is not sanitized before being passed to the QT frontend. This path is used in all components for displaying the server access history. This leads to a rendered HTML4 Subset (QT RichText editor) in the Onionshare frontend. **CVE ID : CVE-2022-21690**	x2v3-v6vq	
Missing Authentication for Critical Function	18-Jan-22	4	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions chat participants can spoof their channel leave message, tricking others into assuming they left the chatroom. **CVE ID : CVE-2022-21691**	https://github.com/onionshare/onionshare/security/advisories/GHSA-w9m4-7w72-r766	A-ONI-ONIO-030222/364
Improper Authentication	18-Jan-22	4	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions anyone with access to the chat environment can write messages disguised as another chat participant. **CVE ID : CVE-2022-21692**	https://github.com/onionshare/onionshare/security/advisories/GHSA-gjj5-998g-v36v	A-ONI-ONIO-030222/365
Improper Limitation of a Pathname to a Restricted Directory	18-Jan-22	4	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions	https://github.com/onionshare/onionshare/security/advisories/GHSA-jgm9-	A-ONI-ONIO-030222/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			an adversary with a primitive that allows for filesystem access from the context of the Onionshare process can access sensitive files in the entire user home folder. This could lead to the leaking of sensitive data. Due to the automatic exclusion of hidden folders, the impact is reduced. This can be mitigated by usage of the flatpak release. **CVE ID : CVE-2022-21693**	xpfj-4fq6	
Incorrect Permission Assignment for Critical Resource	18-Jan-22	5	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. The website mode of the onionshare allows to use a hardened CSP, which will block any scripts and external resources. It is not possible to configure this CSP for individual pages and therefore the security enhancement cannot be used for websites using javascript or external resources like fonts or images. **CVE ID : CVE-2022-21694**	https://github.com/onionshare/onionshare/security/advisories/GHSA-h29c-wcm8-883h	A-ONI-ONIO-030222/367
Improper Authentication	18-Jan-22	5	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions authenticated users (or unauthenticated in public	https://github.com/onionshare/onionshare/security/advisories/GHSA-99p8-9p2c-49j4	A-ONI-ONIO-030222/368

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mode) can send messages without being visible in the list of chat participants. This issue has been resolved in version 2.5. **CVE ID : CVE-2022-21695**		
Improper Input Validation	18-Jan-22	4	OnionShare is an open source tool that lets you securely and anonymously share files, host websites, and chat with friends using the Tor network. In affected versions it is possible to change the username to that of another chat participant with an additional space character at the end of the name string. An adversary with access to the chat environment can use the rename feature to impersonate other participants by adding whitespace characters at the end of the username. **CVE ID : CVE-2022-21696**	https://github.com/onionshare/onionshare/security/advisories/GHSA-68vr-8f46-vc9f	A-ONI-ONIO-030222/369
online_banking_system_project					
online_banking_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jan-22	7.5	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via index.php. **CVE ID : CVE-2022-23363**	N/A	A-ONL-ONLI-030222/370
Oracle					
bi_publisher					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	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, 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 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. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21346**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-BI_P-030222/371
commerce_platform					
N/A	19-Jan-22	5	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.3.0, 11.3.1 and 11.3.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21387**		
communications_billing_and_revenue_management					
N/A	19-Jan-22	5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Pipeline Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Billing and Revenue Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21266**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/373
N/A	19-Jan-22	2.1	Vulnerability in the Oracle	https://ww	A-ORA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Communications Billing and Revenue Management product of Oracle Communications Applications (component: Pipeline Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Communications Billing and Revenue Management executes to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Billing and Revenue Management accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21267**	w.oracle.com/security-alerts/cpujan2022.html	COMM-030222/374
N/A	19-Jan-22	2.1	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Pipeline Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows low privileged attacker with logon to the infrastructure where Oracle Communications Billing and Revenue Management executes to compromise Oracle Communications Billing and Revenue Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Billing and Revenue Management accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21268**		
N/A	19-Jan-22	7.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management,	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21275**		
N/A	19-Jan-22	6.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21276**		
N/A	19-Jan-22	7.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21389**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	7.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Webservices Manager). Supported versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21390**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/379
N/A	19-Jan-22	6.5	Vulnerability in the Oracle Communications Billing and Revenue Management product of Oracle Communications Applications (component: Connection Manager). Supported	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 12.0.0.3 and 12.0.0.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Billing and Revenue Management. While the vulnerability is in Oracle Communications Billing and Revenue Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Communications Billing and Revenue Management. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21391**		
communications_convergence					
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Convergence product of Oracle Communications Applications (component: General Framework). The supported version that is affected is 3.0.2.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/381

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Convergence. 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 Oracle Communications Convergence accessible data as well as unauthorized read access to a subset of Oracle Communications Convergence accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-21338**		
communications_operations_monitor					
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/382

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor 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). **CVE ID : CVE-2022-21246**		
N/A	19-Jan-22	6.5	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks of this vulnerability can result in takeover of Oracle Communications Operations Monitor. CVSS 3.1 Base Score	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21395**		
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor accessible data. CVSS	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/384

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21396**		
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor accessible data. CVSS	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21397**		
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor accessible data. CVSS	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21398**		
N/A	19-Jan-22	6.5	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. While the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Operations	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Monitor. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2022-21399**		
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Monitor 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). **CVE ID : CVE-2022-21400**		
N/A	19-Jan-22	6.5	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. While the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Communications Operations Monitor. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2022-21401**		
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Communications Operations Monitor accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21402**		
N/A	19-Jan-22	6.5	Vulnerability in the Oracle Communications Operations Monitor product of Oracle Communications (component: Mediation Engine). Supported versions that are affected are 3.4, 4.2, 4.3, 4.4 and 5.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Communications Operations Monitor. While the vulnerability is in Oracle Communications Operations Monitor, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Operations Monitor accessible data as well as unauthorized read access to a subset of Oracle Communications Operations Monitor accessible data and unauthorized ability to cause a partial denial of service	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/391

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(partial DOS) of Oracle Communications Operations Monitor. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2022-21403**		
communications_pricing_design_center					
N/A	19-Jan-22	2.1	Vulnerability in the Oracle Communications Pricing Design Center product of Oracle Communications Applications (component: On Premise Install). Supported versions that are affected are 12.0.0.3.0 and 12.0.0.4.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Communications Pricing Design Center executes to compromise Oracle Communications Pricing Design Center. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Communications Pricing Design Center accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21388**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-COMM-030222/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
configurator					
N/A	19-Jan-22	5.5	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: UI Servlet). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Configurator accessible data as well as unauthorized access to critical data or complete access to all Oracle Configurator 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). **CVE ID : CVE-2022-21255**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-CONF-030222/393
database_server					
N/A	19-Jan-22	4	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-DATA-030222/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS 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). **CVE ID : CVE-2022-21247**		
N/A	19-Jan-22	4	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java VM. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21393**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-DATA-030222/395
enterprise_manager_base_platform					
N/A	19-Jan-22	5.5	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager	https://www.oracle.com/security-alerts/cpuja	A-ORA-ENTE-030222/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Policy Framework). Supported versions that are affected are 13.4.0.0 and 13.5.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Enterprise Manager Base Platform accessible data as well as unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 8.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2022-21392**	n2022.html	
enterprise_session_border_controller					
N/A	19-Jan-22	5.5	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications (component: WebUI). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Session Border	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-ENTE-030222/397

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller. While the vulnerability is in Oracle Enterprise Session Border Controller, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Enterprise Session Border Controller accessible data as well as unauthorized read access to a subset of Oracle Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21381**		
N/A	19-Jan-22	4	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications (component: WebUI). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Session Border Controller. While the vulnerability is in Oracle Enterprise Session Border Controller, attacks may significantly impact	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-ENTE-030222/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 7.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N). **CVE ID : CVE-2022-21382**		
N/A	19-Jan-22	4	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications (component: Log). Supported versions that are affected are 8.4 and 9.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Session Border Controller. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Session Border Controller. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21383**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-ENTE-030222/399
graalvm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/400

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g.,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/406

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/408

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-ORA-GRAA-030222/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-ORA-GRAA-030222/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**	om/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpuja	A-ORA-GRAA-030222/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com	A-ORA-GRAA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	030222/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/415

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-GRAA-030222/416

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
installed_base					
N/A	19-Jan-22	7.8	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Instance Main). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Installed Base. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21251**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-INST-030222/417
istore					
N/A	19-Jan-22	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-ISTO-030222/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data as well as unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21354**		
jdk					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21271**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-ORA-JDK-030222/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**	0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.c	A-ORA-JDK-030222/422

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**	om/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported	https://www.oracle.com/security-alerts/cpujan2022.html,	A-ORA-JDK-030222/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21283**	https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM	https://www.oracle.com	A-ORA-JDK-030222/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/432

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JDK-030222/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**		
jre					
N/A	19-Jan-22	4.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-	A-ORA-JRE-030222/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21248**	20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-ORA-JRE-030222/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21277**	rity.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-ORA-JRE-030222/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21282**	alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	
N/A	19-Jan-22	5	Vulnerability in the Oracle	https://ww	A-ORA-JRE-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	030222/439

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21283		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21291**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/441

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21293**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21294**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21296**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21299**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/445

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21305**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/446

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21340**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/447

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21341**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21349**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE,	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/449

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21360**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0007/	A-ORA-JRE-030222/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21365**		
N/A	19-Jan-22	5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-	A-ORA-JRE-030222/451

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21366**	20220121-0007/	
mysql					
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are	https://www.oracle.com/security-alerts/cpujan2022.html,	A-ORA-MYSQ-030222/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 5.7.36 and prior and 8.0.27 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 update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21245**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.27 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21249**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/453

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21253**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/454
N/A	19-Jan-22	6.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21254**		
N/A	19-Jan-22	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21256**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/456
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21264**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21265**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/458
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-ORA-MYSQ-030222/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21270**	alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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 as well as unauthorized update, insert or delete access to some of MySQL Server	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21278**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21279**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/461
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions	https://www.oracle.com/security-alerts/cpuja	A-ORA-MYSQ-030222/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21280**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21284**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21285**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21286**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/465
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory	A-ORA-MYSQ-030222/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21287**	/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker.	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21288**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21289**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/468
N/A	19-Jan-22	4	Vulnerability in the MySQL	https://ww	A-ORA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21290**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	MYSQ-030222/469
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21297**		
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21301**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/471
N/A	19-Jan-22	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior.	https://www.oracle.com/security-alerts/cpujan2022.html,	A-ORA-MYSQ-030222/472

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Difficult to exploit 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 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). **CVE ID : CVE-2022-21302**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21303**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/473

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21304**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/474
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21307**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21308**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/476
N/A	19-Jan-22	4	Vulnerability in the MySQL	https://ww	A-ORA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21309**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	MYSQ-030222/477
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21310**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21311**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/480

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21312**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21313**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/481
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle	https://www.oracle.com	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21314**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/482
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21315**		
N/A	19-Jan-22	4.6	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21316**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21317**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/485
N/A	19-Jan-22	4.6	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster:	https://www.oracle.com/security-	A-ORA-MYSQ-030222/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21318**	alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/487

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21319**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21320**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21321**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/489
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle	https://www.oracle.com	A-ORA-MYSQ-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21322**	/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	030222/490
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21323**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21324**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21325**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21326**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/494
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34	https://www.oracle.com/security-alerts/cpujan2022.html,	A-ORA-MYSQ-030222/495

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21327**	https://security.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/496

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21328**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21329**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21330**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/498
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-ORA-MYSQ-030222/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21331**	0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21332**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21333**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21334**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/502
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior,	https://www.oracle.com/security-alerts/cpujan2022.html, https://secu	A-ORA-MYSQ-030222/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21335**	rity.netapp.com/advisory/ntap-20220121-0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/504

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21336**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21337		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21339**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/506
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21342**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.36 and prior and 8.0.27 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). **CVE ID : CVE-2022-21344**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/508
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-ORA-MYSQ-030222/509

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21348**	0008/	
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21351**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/510
N/A	19-Jan-22	4.9	Vulnerability in the MySQL	https://ww	A-ORA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.26 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 creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2022-21352**	w.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	MYSQ-030222/511
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21355**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/513

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21356**		
N/A	19-Jan-22	2.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2022-21357**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21358**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/515
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2022-21362**		
N/A	19-Jan-22	6	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21363**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-MYSQ-030222/517
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-ORA-MYSQ-030222/518

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21367**	0008/	
N/A	19-Jan-22	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.27 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 as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/519

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server. CVSS 3.1 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2022-21368**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21370**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/520
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-	A-ORA-MYSQ-030222/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21372**	0008/	
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 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). **CVE ID : CVE-2022-21374**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/522
N/A	19-Jan-22	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported	https://www.oracle.com/security-alerts/cpuja	A-ORA-MYSQ-030222/523

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.0.27 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2022-21378**	n2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	
mysql_server					
N/A	19-Jan-22	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 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	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/524

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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). **CVE ID : CVE-2022-21379**		
N/A	19-Jan-22	4	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2022-21380**	https://www.oracle.com/security-alerts/cpujan2022.html, https://security.netapp.com/advisory/ntap-20220121-0008/	A-ORA-MYSQ-030222/525
partner_management					
N/A	19-Jan-22	5.8	Vulnerability in the Oracle Partner Management product	https://www.oracle.com	A-ORA-PART-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Oracle E-Business Suite (component: Reseller Locator). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Partner Management accessible data as well as unauthorized read access to a subset of Oracle Partner Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21373**	/security-alerts/cpujan2022.html	030222/526
peoplesoft_enterprise_cs_sa_integration_pack					
N/A	19-Jan-22	5	Vulnerability in the PeopleSoft Enterprise CS SA Integration Pack product of Oracle PeopleSoft (component: Snapshot Integration). Supported	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PEOP-030222/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS SA Integration Pack. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS SA Integration Pack accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21300**		
peoplesoft_enterprise_peopletools					
N/A	19-Jan-22	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PEOP-030222/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21272**		
N/A	19-Jan-22	4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.58 and 8.59. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PEOP-030222/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21345**		
N/A	19-Jan-22	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Optimization Framework). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PEOP-030222/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21359**		
N/A	19-Jan-22	5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Weblogic). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2022-21364**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PEOP-030222/531
N/A	19-Jan-22	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Rich Text Editor). Supported versions that are affected are 8.57, 8.58 and 8.59. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PEOP-030222/532

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21369**		
primavera_portfolio_management					
N/A	19-Jan-22	4.9	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PRIM-030222/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management 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). **CVE ID : CVE-2022-21242**		
N/A	19-Jan-22	4	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Portfolio Management.	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PRIM-030222/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Primavera Portfolio Management. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2022-21243**		
N/A	19-Jan-22	4.3	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. 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 Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PRIM-030222/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2022-21244**		
N/A	19-Jan-22	5.8	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PRIM-030222/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21269**		
N/A	19-Jan-22	4.9	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2, 20.0.0.0 and 20.0.0.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PRIM-030222/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21281**		
N/A	19-Jan-22	5.8	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2 and 20.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. 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 Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-21376**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PRIM-030222/538
N/A	19-Jan-22	5.8	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and	https://www.oracle.com/security-alerts/cpuja	A-ORA-PRIM-030222/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Engineering (component: Web API). Supported versions that are affected are 18.0.0.0-18.0.3.0, 19.0.0.0-19.0.1.2 and 20.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. 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 Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-21377**	n2022.html	
project_costing					
N/A	19-Jan-22	5.5	Vulnerability in the Oracle Project Costing product of Oracle E-Business Suite (component: Expenses, Currency Override). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-PROJ-030222/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via HTTP to compromise Oracle Project Costing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Project Costing accessible data as well as unauthorized access to critical data or complete access to all Oracle Project Costing 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). **CVE ID : CVE-2022-21273**		
sourcing					
N/A	19-Jan-22	5.5	Vulnerability in the Oracle Sourcing product of Oracle E-Business Suite (component: Intelligence, RFx Creation). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sourcing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sourcing accessible data as well as unauthorized access to critical data or	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-SOUR-030222/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			complete access to all Oracle Sourcing 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). **CVE ID : CVE-2022-21274**		
trade_management					
N/A	19-Jan-22	5.5	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: GL Accounts). Supported versions that are affected are 12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management 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). **CVE ID : CVE-2022-21250**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-TRAD-030222/542
vm_virtualbox					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.32. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2022-21295**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-VM_V-030222/543
N/A	19-Jan-22	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.32. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-VM_V-030222/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2022-21394**		
weblogic_server					
N/A	19-Jan-22	6.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2022-21252**		
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21257		
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). The supported version that is affected is 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21258**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/547
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21259**		
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/549

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21260**		
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server,	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/550

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21261**		
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21262**		
N/A	19-Jan-22	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21292**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/552
N/A	19-Jan-22	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0,	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 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). **CVE ID : CVE-2022-21306**		
N/A	19-Jan-22	6.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2022-21347**		
N/A	19-Jan-22	6.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2022-21350**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/555
N/A	19-Jan-22	6.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2022-21353**		
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21361**		
N/A	19-Jan-22	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2022-21371**	https://www.oracle.com/security-alerts/cpujan2022.html	A-ORA-WEBL-030222/558
N/A	19-Jan-22	5.8	Vulnerability in the Oracle WebLogic Server product of	https://www.oracle.com	A-ORA-WEBL-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2022-21386**	/security-alerts/cpujan2022.html	030222/559
orchardcore					
orchardcore					
Improper Neutralization of Input During Web Page	19-Jan-22	3.5	Cross-site Scripting (XSS) - Stored in NuGet OrchardCore.Application.Cms.Targets prior to 1.2.2.	https://github.com/orchardcms/orchardcore/commit/218f25d	A-ORC-ORCH-030222/560

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-0243**	dfadb66a54de7a82dffe3ab2e4ab7c4b4, https://huntr.dev/bounties/fa538421-ae55-4288-928f-4e96aaed5803	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-22	3.5	Cross-site Scripting (XSS) - Stored in NuGet OrchardCore.Application.Cms.Targets prior to 1.2.2. **CVE ID : CVE-2022-0274**	https://github.com/orchardcms/orchardcore/commit/218f25ddfadb66a54de7a82dffe3ab2e4ab7c4b4, https://huntr.dev/bounties/a82a714a-9b71-475e-bfc3-43326fcaf764	A-ORC-ORCH-030222/561
phoronix-media					
phoronix_test_suite					
Cross-Site Request Forgery (CSRF)	16-Jan-22	4.3	phoronix-test-suite is vulnerable to Cross-Site Request Forgery (CSRF) **CVE ID : CVE-2022-0238**	https://huntr.dev/bounties/63f24b24-4af2-47b8-baea-7ad5f4db3633, https://github.com/phoronix-test-suite/phoron	A-PHO-PHOR-030222/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ix-test-suite/commit/5755b3bf979cd04caa6feee07e403a5be5ac320e	
Phpipam					
phpipam					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-22	3.5	PhpIPAM v1.4.4 allows an authenticated admin user to inject persistent JavaScript code inside the "Site title" parameter while updating the site settings. The "Site title" setting is injected in several locations which triggers the XSS. **CVE ID : CVE-2022-23045**	N/A	A-PHP-PHPI-030222/563
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-22	6.5	PhpIPAM v1.4.4 allows an authenticated admin user to inject SQL sentences in the "subnet" parameter while searching a subnet via app/admin/routing/edit-bgp-mapping-search.php **CVE ID : CVE-2022-23046**	N/A	A-PHP-PHPI-030222/564
Phpmyadmin					
phpmyadmin					
Improper Authentication	22-Jan-22	4	An issue was discovered in phpMyAdmin 4.9 before 4.9.8 and 5.1 before 5.1.2. A valid user who is already authenticated to phpMyAdmin can manipulate their account to bypass two-factor authentication for future login instances.	https://www.phpmyadmin.net/security/PMASA-2022-1/	A-PHP-PHPM-030222/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23807		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-22	4.3	An issue was discovered in phpMyAdmin 5.1 before 5.1.2. An attacker can inject malicious code into aspects of the setup script, which can allow XSS or HTML injection. **CVE ID : CVE-2022-23808**	https://www.phpmyadmin.net/security/PMASA-2022-2/	A-PHP-PHPM-030222/566
Pimcore					
pimcore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-22	3.5	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2022-0256**	https://github.com/pimcore/pimcore/commit/dff1cb0c466abcd55f1268934de3ed937b7436a7, https://huntr.dev/bounties/8d88e48a-7124-4aaf-9f1d-6cfe4f9a79c1	A-PIM-PIMC-030222/567
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-22	3.5	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **CVE ID : CVE-2022-0257**	https://huntr.dev/bounties/bad2073c-bbd5-4425-b3e9-c336b73ddda6, https://github.com/pimcore/pimcore/commit/dfaf78b26fb77990267c0cc05	A-PIM-PIMC-030222/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b9fcb9f8de7b66d	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-22	6.5	pimcore is vulnerable to Improper Neutralization of Special Elements used in an SQL Command **CVE ID : CVE-2022-0258**	https://huntr.dev/bounties/0df891e4-6412-4d9a-a9b7-d9df50311802, https://github.com/pimcore/pimcore/commit/66281c12479dc01a06258d8533eaddfb1770d5bd	A-PIM-PIMC-030222/569
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	3.5	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.2.7. **CVE ID : CVE-2022-0260**	https://huntr.dev/bounties/89e4ab60-21ec-4396-92ad-5b78d4c2897e, https://github.com/pimcore/pimcore/commit/3125d5f0c04cfb5835857ca9416f0bb143130a2f	A-PIM-PIMC-030222/570
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-22	4.3	Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.2.7. **CVE ID : CVE-2022-0262**	https://huntr.dev/bounties/b38a4e14-5dcb-4e49-9990-494dc2a8fa0d, https://githu	A-PIM-PIMC-030222/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				b.com/pimcore/pimcore/commit/6f36e841ce55f67e2e95253dd58f80659ef166c7	
Unrestricted Upload of File with Dangerous Type	18-Jan-22	4.6	Unrestricted Upload of File with Dangerous Type in Packagist pimcore/pimcore prior to 10.2.7. **CVE ID : CVE-2022-0263**	https://huntr.dev/bounties/96506857-06bc-4c84-88b7-4f397715bcf6, https://github.com/pimcore/pimcore/commit/35d1853baf64d6a1d90fd8803e52439da53a3911	A-PIM-PIMC-030222/572
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-22	3.5	Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.2.9. **CVE ID : CVE-2022-0285**	https://github.com/pimcore/pimcore/commit/b432225952e2a5ab0268f401b85a14480369b835, https://huntr.dev/bounties/321918b2-aa01-410e-9f7c-dca5f286bc9c	A-PIM-PIMC-030222/573
rust-lang					
rust					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Jan-22	3.3	Rust is a multi-paradigm, general-purpose programming language designed for performance and safety, especially safe concurrency. The Rust Security Response WG was notified that the \`std::fs::remove_dir_all\` standard library function is vulnerable a race condition enabling symlink following (CWE-363). An attacker could use this security issue to trick a privileged program into deleting files and directories the attacker couldn't otherwise access or delete. Rust 1.0.0 through Rust 1.58.0 is affected by this vulnerability with 1.58.1 containing a patch. Note that the following build targets don't have usable APIs to properly mitigate the attack, and are thus still vulnerable even with a patched toolchain: macOS before version 10.10 (Yosemite) and REDOX. We recommend everyone to update to Rust 1.58.1 as soon as possible, especially people developing programs expected to run in privileged contexts (including system daemons and setuid binaries), as those have the highest risk of being affected by this. Note adding checks in your codebase before calling remove_dir_all	https://github.com/rust-lang/rust/pull/93110, https://github.com/rust-lang/rust/pull/93110/commits/32ed6e599bb4722efefd78bbc9cd7ec4613cb946, https://github.com/rust-lang/rust/pull/93110/commits/406cc071d6cfdfdb678bf3d83d766851de95abaf	A-RUS-RUST-030222/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will not mitigate the vulnerability, as they would also be vulnerable to race conditions like remove_dir_all itself. The existing mitigation is working as intended outside of race conditions. **CVE ID : CVE-2022-21658**		
saviynt					
enterprise_identity_cloud					
Improper Authentication	24-Jan-22	7.5	An issue was discovered in Saviynt Enterprise Identity Cloud (EIC) 5.5 SP2.x. An authentication bypass in ECM/maintenance/forgotpasswordstep1 allows an unauthenticated user to reset passwords and login as any local account. **CVE ID : CVE-2022-23855**	N/A	A-SAV-ENTE-030222/575
Exposure of Resource to Wrong Sphere	24-Jan-22	5	An issue was discovered in Saviynt Enterprise Identity Cloud (EIC) 5.5 SP2.x. An attacker can enumerate users by changing the id parameter, such as for the ECM/maintenance/forgotpasswordstep1 URI. **CVE ID : CVE-2022-23856**	N/A	A-SAV-ENTE-030222/576
Stanford					
corenlp					
Improper Restriction of XML External Entity Reference	17-Jan-22	7.5	corenlp is vulnerable to Improper Restriction of XML External Entity Reference **CVE ID : CVE-2022-0239**	https://huntr.dev/bounties/a717aec2-5646-4a5f-ade0-dadc25736ae3,	A-STA-CORE-030222/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://github.com/stanfordnlp/corenlp/commit/1940ffb938dc4f3f5bc5f2a2fd8b35aabbbae3dd	
starwindsoftware					
command_center					
N/A	24-Jan-22	9	In StarWind Command Center before V2 build 6021, an authenticated read-only user can elevate privileges to administrator through the REST API. **CVE ID : CVE-2022-23858**	https://www.starwindsoftware.com/security/sw-20220121-0001/	A-STA-COMM-030222/578
stormshield					
network_security					
Insertion of Sensitive Information into Log File	17-Jan-22	2.1	In Stormshield SSO Agent 2.x before 2.1.1 and 3.x before 3.0.2, the cleartext user password and PSK are contained in the log file of the .exe installer. **CVE ID : CVE-2022-22703**	https://advisories.stormshield.eu/2022-001	A-STO-NETW-030222/579
teslamate_project					
teslamate					
Improper Authentication	24-Jan-22	7.5	TeslaMate before 1.25.1 (when using the default Docker configuration) allows attackers to open doors of Tesla vehicles, start Keyless Driving, and interfere with vehicle operation en route. This occurs because an attacker can leverage Grafana	https://github.com/adriankumpf/teslamate/commit/fff6915e7364f83b3030f980d5743299c4e5260d,	A-TES-TESL-030222/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			login access to obtain a token for Tesla API calls. **CVE ID : CVE-2022-23126**	https://github.com/adriankumpf/teslamate/releases/tag/v1.25.1, https://github.com/adriankumpf/teslamate/compare/v1.25.0...v1.25.1	
Tibco					
ebx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-22	6	The Web server component of TIBCO Software Inc.'s TIBCO EBX, TIBCO EBX, TIBCO EBX, TIBCO EBX Add-ons, TIBCO EBX Add-ons, TIBCO EBX Add-ons, and TIBCO Product and Service Catalog powered by TIBCO EBX contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 5.8.124 and below, TIBCO EBX: versions 5.9.3, 5.9.4, 5.9.5, 5.9.6, 5.9.7, 5.9.8, 5.9.9, 5.9.10, 5.9.11, 5.9.12, 5.9.13, 5.9.14, and 5.9.15, TIBCO	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/01/tibco-security-advisory-january-19-2022-tibco-ebx-2022-22769	A-TIB-EBX-030222/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EBX: versions 6.0.0, 6.0.1, 6.0.2, and 6.0.3, TIBCO EBX Add-ons: versions 3.20.18 and below, TIBCO EBX Add-ons: versions 4.1.0, 4.2.0, 4.2.1, 4.2.2, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.4.0, 4.4.1, 4.4.2, 4.4.3, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, and 4.5.6, TIBCO EBX Add-ons: versions 5.0.0, 5.0.1, 5.1.0, 5.1.1, and 5.2.0, and TIBCO Product and Service Catalog powered by TIBCO EBX: versions 1.1.0 and below. **CVE ID : CVE-2022-22769**		
ebx_add-ons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-22	6	The Web server component of TIBCO Software Inc.'s TIBCO EBX, TIBCO EBX, TIBCO EBX, TIBCO EBX Add-ons, TIBCO EBX Add-ons, TIBCO EBX Add-ons, and TIBCO Product and Service Catalog powered by TIBCO EBX contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 5.8.124 and below, TIBCO EBX: versions 5.9.3, 5.9.4, 5.9.5,	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/01/tibco-security-advisory-january-19-2022-tibco-ebx-2022-22769	A-TIB-EBX_-030222/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.9.6, 5.9.7, 5.9.8, 5.9.9, 5.9.10, 5.9.11, 5.9.12, 5.9.13, 5.9.14, and 5.9.15, TIBCO EBX: versions 6.0.0, 6.0.1, 6.0.2, and 6.0.3, TIBCO EBX Add-ons: versions 3.20.18 and below, TIBCO EBX Add-ons: versions 4.1.0, 4.2.0, 4.2.1, 4.2.2, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.4.0, 4.4.1, 4.4.2, 4.4.3, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, and 4.5.6, TIBCO EBX Add-ons: versions 5.0.0, 5.0.1, 5.1.0, 5.1.1, and 5.2.0, and TIBCO Product and Service Catalog powered by TIBCO EBX: versions 1.1.0 and below. **CVE ID : CVE-2022-22769**		
product_and_service_catalog_powered_by_tibco_ebx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-22	6	The Web server component of TIBCO Software Inc.'s TIBCO EBX, TIBCO EBX, TIBCO EBX, TIBCO EBX Add-ons, TIBCO EBX Add-ons, TIBCO EBX Add-ons, and TIBCO Product and Service Catalog powered by TIBCO EBX contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/01/tibco-security-advisory-january-19-2022-tibco-ebx-2022-22769	A-TIB-PROD-030222/583

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TIBCO EBX: versions 5.8.124 and below, TIBCO EBX: versions 5.9.3, 5.9.4, 5.9.5, 5.9.6, 5.9.7, 5.9.8, 5.9.9, 5.9.10, 5.9.11, 5.9.12, 5.9.13, 5.9.14, and 5.9.15, TIBCO EBX: versions 6.0.0, 6.0.1, 6.0.2, and 6.0.3, TIBCO EBX Add-ons: versions 3.20.18 and below, TIBCO EBX Add-ons: versions 4.1.0, 4.2.0, 4.2.1, 4.2.2, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.4.0, 4.4.1, 4.4.2, 4.4.3, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, and 4.5.6, TIBCO EBX Add-ons: versions 5.0.0, 5.0.1, 5.1.0, 5.1.1, and 5.2.0, and TIBCO Product and Service Catalog powered by TIBCO EBX: versions 1.1.0 and below. **CVE ID : CVE-2022-22769**		
torchbox					
wagtail					
Exposure of Sensitive Information to an Unauthorized Actor	18-Jan-22	4	Wagtail is a Django based content management system focused on flexibility and user experience. When notifications for new replies in comment threads are sent, they are sent to all users who have replied or commented anywhere on the site, rather than only in the relevant threads. This means that a user could listen in to new comment replies on pages they have not have editing access to, as long as they have left a comment or reply	https://github.com/wagtail/wagtail/commit/5fe901e5d86ed02dbbb63039a897582951266afd, https://github.com/wagtail/wagtail/security/advisories/GHSA-xqxm-2rpm-3889	A-TOR-WAGT-030222/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			somewhere on the site. A patched version has been released as Wagtail 2.15.2, which restores the intended behaviour - to send notifications for new replies to the participants in the active thread only (editing permissions are not considered). New comments can be disabled by setting `WAGTAILADMIN_COMMENTS_ENABLED = False` in the Django settings file. **CVE ID : CVE-2022-21683**		
Trendmicro					
deep_security_agent					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jan-22	4.3	A directory traversal vulnerability in Trend Micro Deep Security and Cloud One - Workload Security Agent for Linux version 20 and below could allow an attacker to read arbitrary files from the file system. Please note: an attacker must first obtain compromised access to the target Deep Security Manager (DSM) or the target agent must be not yet activated or configured in order to exploit this vulnerability. **CVE ID : CVE-2022-23119**	https://success.trendmicro.com/solution/000290104	A-TRE-DEEP-030222/585
Improper Control of Generation of Code ('Code Injection')	20-Jan-22	6.9	A code injection vulnerability in Trend Micro Deep Security and Cloud One - Workload Security Agent for Linux version 20 and below could allow an attacker to escalate	https://success.trendmicro.com/solution/000290104	A-TRE-DEEP-030222/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges and run arbitrary code in the context of root. Please note: an attacker must first obtain access to the target agent in an un-activated and unconfigured state in order to exploit this vulnerability. **CVE ID : CVE-2022-23120**		
Umbraco					
umbraco_cms					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	18-Jan-22	5	Within the Umbraco CMS, a configuration element named "UmbracoApplicationUrl" (or just "ApplicationUrl") is used whenever application code needs to build a URL pointing back to the site. For example, when a user resets their password and the application builds a password reset URL or when the administrator invites users to the site. For Umbraco versions less than 9.2.0, if the Application URL is not specifically configured, the attacker can manipulate this value and store it persistently affecting all users for components where the "UmbracoApplicationUrl" is used. For example, the attacker is able to change the URL users receive when resetting their password so that it points to the attackers server, when the user follows this link the reset token can be intercepted by the attacker resulting in account	N/A	A-UMB-UMBR-030222/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			takeover. **CVE ID : CVE-2022-22690**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	18-Jan-22	4.3	The password reset component deployed within Umbraco uses the hostname supplied within the request host header when building a password reset URL. It may be possible to manipulate the URL sent to Umbraco users when so that it points to the attackers server thereby disclosing the password reset token if/when the link is followed. A related vulnerability (CVE-2022-22690) could allow this flaw to become persistent so that all password reset URLs are affected persistently following a successful attack. See the AppCheck advisory for further information and associated caveats. **CVE ID : CVE-2022-22691**	N/A	A-UMB-UMBR-030222/588
usbview_project					
usbview					
Improper Authentication	21-Jan-22	7.2	USBView 2.1 before 2.2 allows some local users (e.g., ones logged in via SSH) to execute arbitrary code as root because certain Polkit settings (e.g., allow_any=yes) for pkexec disable the authentication requirement. Code execution can, for example, use the --gtk-module option. This affects Ubuntu, Debian, and Gentoo.	https://github.com/gregkh/usbview/commit/bf374fa4e5b9a756789dfd88efa93806a395463b, https://www.openwall.com/lists/oss-	A-USB-USBV-030222/589

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23220	security/2022/01/21/1	
VIM					
vim					
Heap-based Buffer Overflow	18-Jan-22	6.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-0261**	https://github.com/vim/vim/commit/9f8c304c8a390ade133bac29963dc8e56ab14cbc, https://huntr.dev/bounties/fa795954-8775-4f23-98c6-d4d4d3fe8a82	A-VIM-VIM-030222/590
Heap-based Buffer Overflow	21-Jan-22	7.5	Heap-based Buffer Overflow in vim/vim prior to 8.2. **CVE ID : CVE-2022-0318**	https://github.com/vim/vim/commit/57df9e8a9f9ae1aafdde9b86b10ad907627a87dc, https://huntr.dev/bounties/0d10ba02-b138-4e68-a284-67f781a62d08	A-VIM-VIM-030222/591
Out-of-bounds Read	21-Jan-22	4.3	Out-of-bounds Read in vim/vim prior to 8.2. **CVE ID : CVE-2022-0319**	https://huntr.dev/bounties/ba622fd2-e6ef-4ad9-95b4-17f87b68755b,	A-VIM-VIM-030222/592

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://github.com/vim/vim/commit/05b27615481e72e3b338bb12990fb3e0c2ecc2a9	
Access of Memory Location Before Start of Buffer	25-Jan-22	4.6	Access of Memory Location Before Start of Buffer in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-0351**	https://github.com/vim/vim/commit/fe6fb267e6ee5c5da2f41889e4e0e0ac5bf4b89d, https://huntr.dev/bounties/8b36db58-b65c-4298-be7f-40b9e37fd161	A-VIM-VIM-030222/593
vjinfotech					
wp_import_export					
Missing Authorization	18-Jan-22	5	The WP Import Export WordPress plugin (both free and premium versions) is vulnerable to unauthenticated sensitive data disclosure due to a missing capability check on the download function wpie_process_file_download found in the ~/includes/classes/class-wpie-general.php file. This made it possible for unauthenticated attackers to download any imported or exported information from a vulnerable site which can	https://plugins.trac.wordpress.org/changeset/2649762/wp-import-export-lite/trunk/includes/classes/class-wpie-general.php	A-VJI-WP_I-030222/594

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contain sensitive information like user data. This affects versions up to, and including, 3.9.15. **CVE ID : CVE-2022-0236**		
wp_import_export_lite					
Missing Authorization	18-Jan-22	5	The WP Import Export WordPress plugin (both free and premium versions) is vulnerable to unauthenticated sensitive data disclosure due to a missing capability check on the download function wpie_process_file_download found in the ~/includes/classes/class-wpie-general.php file. This made it possible for unauthenticated attackers to download any imported or exported information from a vulnerable site which can contain sensitive information like user data. This affects versions up to, and including, 3.9.15. **CVE ID : CVE-2022-0236**	https://plugins.trac.wordpress.org/changeset/2649762/wp-import-export-lite/trunk/includes/classes/class-wpie-general.php	A-VJI-WP_I-030222/595
W1.fi					
hostapd					
Observable Discrepancy	17-Jan-22	6.8	The implementations of SAE in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-	https://w1.fi/security/2022-1/	A-W1.-HOST-030222/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9494. **CVE ID : CVE-2022-23303**		
Observable Discrepancy	17-Jan-22	6.8	The implementations of EAP-pwd in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side-channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9495. **CVE ID : CVE-2022-23304**	https://w1.fi/security/2022-1/	A-W1.-HOST-030222/597
wpa_supplicant					
Observable Discrepancy	17-Jan-22	6.8	The implementations of SAE in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9494. **CVE ID : CVE-2022-23303**	https://w1.fi/security/2022-1/	A-W1.-WPA_-030222/598
Observable Discrepancy	17-Jan-22	6.8	The implementations of EAP-pwd in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side-channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9495. **CVE ID : CVE-2022-23304**	https://w1.fi/security/2022-1/	A-W1.-WPA_-030222/599
wasmcloud					
host_runtime					
Incorrect Authorizatio	21-Jan-22	5.5	wasmCloud Host Runtime is a server process that securely hosts and provides dispatch	https://github.com/wasmCloud/wasm	A-WAS-HOST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			for web assembly (WASM) actors and capability providers. In versions prior to 0.52.2 actors can bypass capability authorization. Actors are normally required to declare their capabilities for inbound invocations, but with this vulnerability actor capability claims are not verified upon receiving invocations. This compromises the security model for actors as they can receive unauthorized invocations from linked capability providers. The problem has been patched in versions `0.52.2` and greater. There is no workaround and users are advised to upgrade to an unaffected version as soon as possible. **CVE ID : CVE-2022-21707**	cloud-otp/security/advisories/GHSA-2cmx-rr54-88g5, https://github.com/wasmCloud/wasmcloud-otp/commit/fd07262074b98b06106a31fd1957dc2319d438a5	030222/600
Wolfssl					
wolfssl					
Use of Insufficiently Random Values	18-Jan-22	6.4	wolfSSL 5.x before 5.1.1 uses non-random IV values in certain situations. This affects connections (without AEAD) using AES-CBC or DES3 with TLS 1.1 or 1.2 or DTLS 1.1 or 1.2. This occurs because of misplaced memory initialization in BuildMessage in internal.c. **CVE ID : CVE-2022-23408**	N/A	A-WOL-WOLF-030222/601
xootix					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
login\\/signup_popup					
Cross-Site Request Forgery (CSRF)	18-Jan-22	6.8	The Login/Signup Popup, Waitlist Woocommerce (Back in stock notifier), and Side Cart Woocommerce (Ajax) WordPress plugins by XootiX are vulnerable to Cross-Site Request Forgery via the save_settings function found in the ~/includes/xoo-framework/admin/class-xoo-admin-settings.php file which makes it possible for attackers to update arbitrary options on a site that can be used to create an administrative user account and grant full privileged access to a compromised site. This affects versions <= 2.2 in Login/Signup Popup, versions <= 2.5.1 in Waitlist Woocommerce (Back in stock notifier), and versions <= 2.0 in Side Cart Woocommerce (Ajax). **CVE ID : CVE-2022-0215**	N/A	A-XOO-LOGI-030222/602
side_cart_woocommerce					
Cross-Site Request Forgery (CSRF)	18-Jan-22	6.8	The Login/Signup Popup, Waitlist Woocommerce (Back in stock notifier), and Side Cart Woocommerce (Ajax) WordPress plugins by XootiX are vulnerable to Cross-Site Request Forgery via the save_settings function found in the ~/includes/xoo-framework/admin/class-xoo-admin-settings.php file which makes it possible for	N/A	A-XOO-SIDE-030222/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to update arbitrary options on a site that can be used to create an administrative user account and grant full privileged access to a compromised site. This affects versions <= 2.2 in Login/Signup Popup, versions <= 2.5.1 in Waitlist Woocommerce (Back in stock notifier), and versions <= 2.0 in Side Cart Woocommerce (Ajax). **CVE ID : CVE-2022-0215**		
waitlist_woocommerce					
Cross-Site Request Forgery (CSRF)	18-Jan-22	6.8	The Login/Signup Popup, Waitlist Woocommerce (Back in stock notifier), and Side Cart Woocommerce (Ajax) WordPress plugins by XootiX are vulnerable to Cross-Site Request Forgery via the save_settings function found in the ~/includes/xoo-framework/admin/class-xoo-admin-settings.php file which makes it possible for attackers to update arbitrary options on a site that can be used to create an administrative user account and grant full privileged access to a compromised site. This affects versions <= 2.2 in Login/Signup Popup, versions <= 2.5.1 in Waitlist Woocommerce (Back in stock notifier), and versions <= 2.0 in Side Cart Woocommerce (Ajax).	N/A	A-XOO-WAIT-030222/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0215		
yetiforce					
yetiforce_customer_relationship_management					
Cross-Site Request Forgery (CSRF)	24-Jan-22	6	Cross-Site Request Forgery (CSRF) in Packagist yetiforce/yetiforce-crm prior to 6.3.0. **CVE ID : CVE-2022-0269**	https://huntr.dev/bounties/a0470915-f6df-45b8-b3a2-01aebe764df0, https://github.com/yetiforcecompany/yetiforcecrm/commit/298c7870e6fe4332d8aa1757a9c8d79f841389ff	A-YET-YETI-030222/605
Hardware					
Asus					
pa90					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PA90-030222/606
pb50					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system	https://www.twcert.org.tw/tw/cp-132-5547-	H-ASU-PB50-030222/607

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	34bc4-1.html	
pb60					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PB60-030222/608
pb60g					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PB60-030222/609
pb60s					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI)	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PB60-030222/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**		
pb60v					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PB60-030222/611
pb61v					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PB61-030222/612
pn30					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PN30-030222/613

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**		
pn40					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PN40-030222/614
pn60					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-PN60-030222/615
ts10					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service.	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-TS10-030222/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21933		
un65u					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-UN65-030222/617
vc65-c1					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	H-ASU-VC65-030222/618
Juniper					
acx5448					
Uncontrolled Resource Consumption	19-Jan-22	3.3	An Uncontrolled Resource Consumption vulnerability in the handling of IPv6 neighbor state change events in Juniper Networks Junos OS allows an adjacent attacker to cause a memory leak in the Flexible PIC Concentrator (FPC) of an ACX5448 router. The continuous flapping of an IPv6 neighbor with specific	https://kb.juniper.net/JSA11263	H-JUN-ACX5-030222/619

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			timing will cause the FPC to run out of resources, leading to a Denial of Service (DoS) condition. Once the condition occurs, further packet processing will be impacted, creating a sustained Denial of Service (DoS) condition, requiring a manual PFE restart to restore service. The following error messages will be seen after the FPC resources have been exhausted: fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 fpc0		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 This issue only affects the ACX5448 router. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS on ACX5448: 18.4 versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S8, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. **CVE ID : CVE-2022-22155**		
mx10					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit	https://kb.juniper.net/JSA11261	H-JUN-MX10-030222/620

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-	https://kb.juniper.net/JSA11268	H-JUN-MX10-030222/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1,	https://kb.juniper.net/JSA11281	H-JUN-MX10-030222/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-MX10-030222/623
mx10000					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources	https://kb.juniper.net/JSA11261	H-JUN-MX10-030222/624

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and	https://kb.juniper.net/JSA11268	H-JUN-MX10-030222/625

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are	https://kb.juniper.net/JSA11281	H-JUN-MX10-030222/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3	https://kb.juniper.net/JSA11284	H-JUN-MX10-030222/627

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx10003					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-MX10-030222/628
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper	https://kb.juniper.net/JSA11268	H-JUN-MX10-030222/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause	https://kb.juniper.net/JSA11281	H-JUN-MX10-030222/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if	https://kb.juniper.net/JSA11284	H-JUN-MX10-030222/631

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx10008					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions	https://kb.juniper.net/JSA11261	H-JUN-MX10-030222/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper	https://kb.juniper.net/JSA11268	H-JUN-MX10-030222/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-MX10-030222/634
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked	https://kb.juniper.net/JSA11284	H-JUN-MX10-030222/635

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx10016					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of	https://kb.juniper.net/JSA11261	H-JUN-MX10-030222/636

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions	https://kb.juniper.net/JSA11268	H-JUN-MX10-030222/637

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos	https://kb.juniper.net/JSA11281	H-JUN-MX10-030222/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-MX10-030222/639
mx104					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow	https://kb.juniper.net/JSA11261	H-JUN-MX10-030222/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific	https://kb.juniper.net/JSA11268	H-JUN-MX10-030222/641

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue	https://kb.juniper.net/JSA11281	H-JUN-MX10-030222/642

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper	https://kb.juniper.net/JSA11284	H-JUN-MX10-030222/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx150					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-MX15-030222/644
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent	https://kb.juniper.net/JSA11268	H-JUN-MX15-030222/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a	https://kb.juniper.net/JSA11281	H-JUN-MX15-030222/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted	https://kb.juniper.net/JSA11284	H-JUN-MX15-030222/647

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx2008					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2;	https://kb.juniper.net/JSA11261	H-JUN-MX20-030222/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.	https://kb.juniper.net/JSA11268	H-JUN-MX20-030222/649

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22160		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-MX20-030222/650
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of	https://kb.juniper.net/JSA11284	H-JUN-MX20-030222/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx2010					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high	https://kb.juniper.net/JSA11261	H-JUN-MX20-030222/652

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3;	https://kb.juniper.net/JSA11268	H-JUN-MX20-030222/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-MX20-030222/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-MX20-030222/655
mx2020					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series	https://kb.juniper.net/JSA11261	H-JUN-MX20-030222/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version	https://kb.juniper.net/JSA11268	H-JUN-MX20-030222/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions	https://kb.juniper.net/JSA11281	H-JUN-MX20-030222/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-MX20-030222/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mx204					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-MX20-030222/660
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband	https://kb.juniper.net/JSA11268	H-JUN-MX20-030222/661

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service	https://kb.juniper.net/JSA11281	H-JUN-MX20-030222/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4	https://kb.juniper.net/JSA11284	H-JUN-MX20-030222/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx240					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-MX24-030222/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**	https://kb.juniper.net/JSA11268	H-JUN-MX24-030222/665
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG	https://kb.juniper.net/JS	H-JUN-MX24-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	A11281	030222/666
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained	https://kb.juniper.net/JSA11284	H-JUN-MX24-030222/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx40					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks	https://kb.juniper.net/JSA11261	H-JUN-MX40-030222/668

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4	https://kb.juniper.net/JSA11268	H-JUN-MX40-030222/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-MX40-030222/670
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon	https://kb.juniper.net/JSA11284	H-JUN-MX40-030222/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx480					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in	https://kb.juniper.net/JSA11261	H-JUN-MX48-030222/672

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3,	https://kb.juniper.net/JSA11268	H-JUN-MX48-030222/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to	https://kb.juniper.net/JSA11281	H-JUN-MX48-030222/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-MX48-030222/675
mx5					
Inefficient	19-Jan-22	5	An Insufficient Algorithmic	https://kb.ju	H-JUN-MX5-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Algorithmic Complexity			Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	niper.net/JSA11261	030222/676
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration	https://kb.juniper.net/JSA11268	H-JUN-MX5-030222/677

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the	https://kb.juniper.net/JSA11281	H-JUN-MX5-030222/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to	https://kb.juniper.net/JSA11284	H-JUN-MX5-030222/679

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx80					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-MX80-030222/680
Unchecked Error	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the	https://kb.juniper.net/JS	H-JUN-MX80-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition			subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**	A11268	030222/681
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series	https://kb.juniper.net/JSA11281	H-JUN-MX80-030222/682

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by	https://kb.juniper.net/JSA11284	H-JUN-MX80-030222/683

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
mx960					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions	https://kb.juniper.net/JSA11261	H-JUN-MX96-030222/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2	https://kb.juniper.net/JSA11268	H-JUN-MX96-030222/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-MX96-030222/686
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and	https://kb.juniper.net/JSA11284	H-JUN-MX96-030222/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx100					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit	https://kb.juniper.net/JSA11261	H-JUN-SRX1-030222/688

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set	https://kb.juniper.net/JSA11265	H-JUN-SRX1-030222/689

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are	https://kb.juniper.net/JSA11281	H-JUN-SRX1-030222/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3	https://kb.juniper.net/JSA11284	H-JUN-SRX1-030222/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx110					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX1-030222/692
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways	https://kb.juniper.net/JSA11265	H-JUN-SRX1-030222/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-SRX1-030222/694
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked	https://kb.juniper.net/JSA11284	H-JUN-SRX1-030222/695

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx1400					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of	https://kb.juniper.net/JSA11261	H-JUN-SRX1-030222/696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on	https://kb.juniper.net/JSA11265	H-JUN-SRX1-030222/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue	https://kb.juniper.net/JSA11281	H-JUN-SRX1-030222/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper	https://kb.juniper.net/JSA11284	H-JUN-SRX1-030222/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx1500					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX1-030222/700
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet	https://kb.juniper.net/JSA11265	H-JUN-SRX1-030222/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1.		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22167		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-SRX1-030222/702
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of	https://kb.juniper.net/JSA11284	H-JUN-SRX1-030222/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx210					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high	https://kb.juniper.net/JSA11261	H-JUN-SRX2-030222/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS	https://kb.juniper.net/JSA11265	H-JUN-SRX2-030222/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and	https://kb.juniper.net/JSA11281	H-JUN-SRX2-030222/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1.	https://kb.juniper.net/JSA11284	H-JUN-SRX2-030222/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22178		
srx220					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX2-030222/708
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when	https://kb.juniper.net/JSA11265	H-JUN-SRX2-030222/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper	19-Jan-22	4.3	An Improper Locking	https://kb.ju	H-JUN-SRX2-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Locking			vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	niper.net/JSA11281	030222/710
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific	https://kb.juniper.net/JSA11284	H-JUN-SRX2-030222/711

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx240					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue	https://kb.juniper.net/JSA11261	H-JUN-SRX2-030222/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-	https://kb.juniper.net/JSA11265	H-JUN-SRX2-030222/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1	https://kb.juniper.net/JSA11281	H-JUN-SRX2-030222/714

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX2-030222/715
srx240h2					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX2-030222/716
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI	https://kb.juniper.net/JSA11265	H-JUN-SRX2-030222/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS	https://kb.juniper.net/JSA11281	H-JUN-SRX2-030222/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition.	https://kb.juniper.net/JSA11284	H-JUN-SRX2-030222/719

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx300					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX	https://kb.juniper.net/JSA11261	H-JUN-SRX3-030222/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/721

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/722

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/723
srx320					
Inefficient	19-Jan-22	5	An Insufficient Algorithmic	https://kb.ju	H-JUN-SRX3-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Algorithmic Complexity			Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	niper.net/JSA11261	030222/724
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/726

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx340					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions	https://kb.juniper.net/JSA11261	H-JUN-SRX3-030222/728

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/730

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/731
srx3400					
Inefficient Algorithmic	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an	https://kb.juniper.net/JS	H-JUN-SRX3-030222/732

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Complexity			Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	A11261	
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/733

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/734

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx345					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions	https://kb.juniper.net/JSA11261	H-JUN-SRX3-030222/736

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1,	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/738

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/739
srx3600					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources	https://kb.juniper.net/JSA11261	H-JUN-SRX3-030222/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/743

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx380					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions	https://kb.juniper.net/JSA11261	H-JUN-SRX3-030222/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions	https://kb.juniper.net/JSA11265	H-JUN-SRX3-030222/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not	https://kb.juniper.net/JSA11281	H-JUN-SRX3-030222/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX3-030222/747
srx4000					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling	https://kb.juniper.net/JSA11261	H-JUN-SRX4-030222/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification	https://kb.juniper.net/JSA11265	H-JUN-SRX4-030222/749

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon	https://kb.juniper.net/JSA11281	H-JUN-SRX4-030222/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to	https://kb.juniper.net/JSA11284	H-JUN-SRX4-030222/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx4100					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3;	https://kb.juniper.net/JSA11261	H-JUN-SRX4-030222/752

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1	https://kb.juniper.net/JSA11265	H-JUN-SRX4-030222/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos	https://kb.juniper.net/JSA11281	H-JUN-SRX4-030222/754

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX4-030222/755
srx4200					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow	https://kb.juniper.net/JSA11261	H-JUN-SRX4-030222/756

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorizatio n	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy	https://kb.juniper.net/JSA11265	H-JUN-SRX4-030222/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a	https://kb.juniper.net/JSA11281	H-JUN-SRX4-030222/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted	https://kb.juniper.net/JSA11284	H-JUN-SRX4-030222/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx4600					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2;	https://kb.juniper.net/JSA11261	H-JUN-SRX4-030222/760

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1;	https://kb.juniper.net/JSA11265	H-JUN-SRX4-030222/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1.	https://kb.juniper.net/JSA11281	H-JUN-SRX4-030222/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22175		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	https://kb.juniper.net/JSA11284	H-JUN-SRX4-030222/763
srx5000					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/764

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the	https://kb.juniper.net/JSA11265	H-JUN-SRX5-030222/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This	https://kb.juniper.net/JSA11284	H-JUN-SRX5-030222/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx5400					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2.	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22153		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4	https://kb.juniper.net/JSA11265	H-JUN-SRX5-030222/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/770
Stack-based Buffer	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the	https://kb.juniper.net/JS	H-JUN-SRX5-030222/771

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**	A11284	
srx550					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/772

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to	https://kb.juniper.net/JSA11265	H-JUN-SRX5-030222/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/774

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2;	https://kb.juniper.net/JSA11284	H-JUN-SRX5-030222/775

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx550m					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/776
Incorrect	19-Jan-22	6.8	A traffic classification	https://kb.ju	H-JUN-SRX5-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to	niper.net/JSA11265	030222/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/778
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks	https://kb.juniper.net/JSA11284	H-JUN-SRX5-030222/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx550_hm					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue	https://kb.juniper.net/JSA11265	H-JUN-SRX5-030222/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2	https://kb.juniper.net/JSA11284	H-JUN-SRX5-030222/783

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx5600					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/784
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the	https://kb.juniper.net/JSA11265	H-JUN-SRX5-030222/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/786
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an	https://kb.juniper.net/JSA11284	H-JUN-SRX5-030222/787

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx5800					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant	https://kb.juniper.net/JSA11261	H-JUN-SRX5-030222/788

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-	https://kb.juniper.net/JSA11265	H-JUN-SRX5-030222/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed	https://kb.juniper.net/JSA11281	H-JUN-SRX5-030222/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This	https://kb.juniper.net/JSA11284	H-JUN-SRX5-030222/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
srx650					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**	https://kb.juniper.net/JSA11261	H-JUN-SRX6-030222/792
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to	https://kb.juniper.net/JSA11265	H-JUN-SRX6-030222/793

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**	https://kb.juniper.net/JSA11281	H-JUN-SRX6-030222/794
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd	https://kb.juniper.net/JSA11284	H-JUN-SRX6-030222/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
kingjim					
mirupass_pw10					
Missing Encryption of Sensitive Data	17-Jan-22	2.1	Missing encryption of sensitive data vulnerability in 'MIRUPASS' PW10 firmware all versions and 'MIRUPASS' PW20 firmware all versions allows an attacker who can physically access the device to obtain the stored passwords. **CVE ID : CVE-2022-0183**	https://www.kingjim.co.jp/download/security/#mirupass	H-KIN-MIRU-030222/796
mirupass_pw20					
Missing Encryption of Sensitive	17-Jan-22	2.1	Missing encryption of sensitive data vulnerability in 'MIRUPASS' PW10 firmware	https://www.kingjim.co.jp/download	H-KIN-MIRU-030222/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			all versions and 'MIRUPASS' PW20 firmware all versions allows an attacker who can physically access the device to obtain the stored passwords. **CVE ID : CVE-2022-0183**	/security/#mirupass	
spc10					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	https://www.kingjim.co.jp/download/security/#sr01	H-KIN-SPC1-030222/798
tepura_pro_sr-7900p					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	https://www.kingjim.co.jp/download/security/#sr01	H-KIN-TEPU-030222/799
tepura_pro_sr5900p					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and	https://www.kingjim.co.jp/download/security/#s	H-KIN-TEPU-030222/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	r01	
Operating System					
Apple					
macos					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-APP-MACO-030222/801
Asus					
pa90_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PA90-030222/802
pb50_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PB50-030222/803
pb60g_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PB60-030222/804
pb60s_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PB60-030222/805
pb60v_firmware					
Improper Input	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input	https://www.twcert.org.	O-ASU-PB60-030222/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	tw/tw/cp-132-5547-34bc4-1.html	
pb60_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PB60-030222/807
pb61v_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PB61-030222/808
pn30_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system	https://www.twcert.org.tw/tw/cp-132-5547-	O-ASU-PN30-030222/809

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	34bc4-1.html	
pn40_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PN40-030222/810
pn60_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-PN60-030222/811
ts10_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI)	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-TS10-030222/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**		
un65u_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-UN65-030222/813
vc65-c1_firmware					
Improper Input Validation	21-Jan-22	7.2	ASUS VivoMini/Mini PC device has an improper input validation vulnerability. A local attacker with system privilege can use system management interrupt (SMI) to modify memory, resulting in arbitrary code execution for controlling the system or disrupting service. **CVE ID : CVE-2022-21933**	https://www.twcert.org.tw/tw/cp-132-5547-34bc4-1.html	O-ASU-VC65-030222/814
Canonical					
ubuntu_linux					
Improper Authentication	21-Jan-22	7.2	USBView 2.1 before 2.2 allows some local users (e.g., ones logged in via SSH) to execute arbitrary code as root because certain Polkit settings (e.g., allow_any=yes) for pkexec disable the	https://github.com/gregkh/usbview/commit/bf374fa4e5b9a756789dfd88efa93806a395	O-CAN-UBUN-030222/815

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication requirement. Code execution can, for example, use the --gtk-module option. This affects Ubuntu, Debian, and Gentoo. **CVE ID : CVE-2022-23220**	463b, https://www.openwall.com/lists/oss-security/2022/01/21/1	
Out-of-bounds Read	21-Jan-22	4.3	Out-of-bounds Read in vim/vim prior to 8.2. **CVE ID : CVE-2022-0319**	https://huntr.dev/bounties/ba622fd2-e6ef-4ad9-95b4-17f87b68755b, https://github.com/vim/vim/commit/05b27615481e72e3b338bb12990fb3e0c2ecc2a9	O-CAN-UBUN-030222/816
Debian					
debian_linux					
Improper Privilege Management	19-Jan-22	4.6	IPython (Interactive Python) is a command shell for interactive computing in multiple programming languages, originally developed for the Python programming language. Affected versions are subject to an arbitrary code execution vulnerability achieved by not properly managing cross user temporary files. This vulnerability allows one user to run code as another on the same machine. All users are	https://github.com/ipython/ipython/security/advisories/GHSA-pq7m-3gw7-gq5x, https://github.com/ipython/ipython/commit/46a51ed69cdf41b4333943d9ceeb945c4ede5668	O-DEB-DEBI-030222/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advised to upgrade. **CVE ID : CVE-2022-21699**		
Improper Authentication	21-Jan-22	7.2	USBView 2.1 before 2.2 allows some local users (e.g., ones logged in via SSH) to execute arbitrary code as root because certain Polkit settings (e.g., allow_any=yes) for pkexec disable the authentication requirement. Code execution can, for example, use the --gtk-module option. This affects Ubuntu, Debian, and Gentoo. **CVE ID : CVE-2022-23220**	https://github.com/gregkh/usbview/commit/bf374fa4e5b9a756789dfd88efa93806a395463b, https://www.openwall.com/lists/oss-security/2022/01/21/1	O-DEB-DEBI-030222/818
Fedoraproject					
fedora					
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Jan-22	3.3	Rust is a multi-paradigm, general-purpose programming language designed for performance and safety, especially safe concurrency. The Rust Security Response WG was notified that the `std::fs::remove_dir_all` standard library function is vulnerable a race condition enabling symlink following (CWE-363). An attacker could use this security issue to trick a privileged program into deleting files and directories the attacker couldn't otherwise access or delete. Rust 1.0.0 through Rust 1.58.0 is affected by this vulnerability with 1.58.1	https://github.com/rust-lang/rust/pull/93110, https://github.com/rust-lang/rust/pull/93110/commits/32ed6e599bb4722efefd78bbc9cd7ec4613cb946, https://github.com/rust-lang/rust/pull/93110/commits/406cc071d6cfdfdb678bf3d83d766851de95	O-FED-FEDO-030222/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			containing a patch. Note that the following build targets don't have usable APIs to properly mitigate the attack, and are thus still vulnerable even with a patched toolchain: macOS before version 10.10 (Yosemite) and REDOX. We recommend everyone to update to Rust 1.58.1 as soon as possible, especially people developing programs expected to run in privileged contexts (including system daemons and setuid binaries), as those have the highest risk of being affected by this. Note that adding checks in your codebase before calling remove_dir_all will not mitigate the vulnerability, as they would also be vulnerable to race conditions like remove_dir_all itself. The existing mitigation is working as intended outside of race conditions. **CVE ID : CVE-2022-21658**	abaf	
Gentoo					
linux					
Improper Authentication	21-Jan-22	7.2	USBView 2.1 before 2.2 allows some local users (e.g., ones logged in via SSH) to execute arbitrary code as root because certain Polkit settings (e.g., allow_any=yes) for pkexec disable the authentication requirement. Code execution can, for example, use the --gtk-	https://github.com/gregkh/usbview/commit/bf374fa4e5b9a756789dfd88efa93806a395463b, https://www.openwall.c	O-GEN-LINU-030222/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			module option. This affects Ubuntu, Debian, and Gentoo. **CVE ID : CVE-2022-23220**	om/lists/oss-security/2022/01/21/1	
Google					
android					
N/A	21-Jan-22	9.4	Attacker can reset the device with AT Command in the process of rebooting the device. The LG ID is LVE-SMP-210011. **CVE ID : CVE-2022-23728**	https://lgsecurity.lge.com/bulletins/mobile	O-GOO-ANDR-030222/821
HP					
hp-ux					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-HP-HP-U-030222/822
IBM					
aix					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541	O-IBM-AIX-030222/823

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	530	
i					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-IBM-I-030222/824
z\\/os					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-IBM-Z\\/-030222/825
Juniper					
junos					
Inefficient Algorithmic Complexity	19-Jan-22	5	An Insufficient Algorithmic Complexity combined with an Allocation of Resources Without Limits or Throttling vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS	https://kb.juniper.net/JSA11261	O-JUN-JUNO-030222/826

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series and MX Series with SPC3 allows an unauthenticated network attacker to cause latency in transit packet processing and even packet loss. If transit traffic includes a significant percentage (> 5%) of fragmented packets which need to be reassembled, high latency or packet drops might be observed. This issue affects Juniper Networks Junos OS on SRX Series, MX Series with SPC3: All versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2-S9, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2022-22153**		
Exposure of Resource to Wrong Sphere	19-Jan-22	4.6	In a Junos Fusion scenario an External Control of Critical State Data vulnerability in the Satellite Device (SD) control state machine of Juniper Networks Junos OS allows an attacker who is able to make physical changes to the cabling of the device to cause a denial of service (DoS). An SD can get rebooted and subsequently controlled by an Aggregation Device (AD) which does not belong to the original Fusion setup and is just connected to an extended port of the SD. To carry out this attack the attacker needs	https://kb.juniper.net/JSA11262	O-JUN-JUNO-030222/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to have physical access to the cabling between the SD and the original AD. This issue affects: Juniper Networks Junos OS 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S4. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22154**		
Uncontrolled Resource Consumption	19-Jan-22	3.3	An Uncontrolled Resource Consumption vulnerability in the handling of IPv6 neighbor state change events in Juniper Networks Junos OS allows an adjacent attacker to cause a memory leak in the Flexible PIC Concentrator (FPC) of an ACX5448 router. The continuous flapping of an IPv6 neighbor with specific timing will cause the FPC to run out of resources, leading to a Denial of Service (DoS) condition. Once the condition occurs, further packet processing will be impacted, creating a sustained Denial of Service (DoS) condition, requiring a manual PFE restart to restore service. The following error messages will be seen after the FPC resources have been exhausted: fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135:	https://kb.juniper.net/JSA11263	O-JUN-JUNO-030222/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 fpc0 DNX_NH::dnx_nh_tag_ipv4_hw_install(),3135: dnx_nh_tag_ipv4_hw_install: BCM L3 Egress create object failed for NH 602 (-14:No resources for operation), BCM NH Params: unit:0 Port:41, L3_INTF:0 Flags: 0x40 This issue only affects the ACX5448 router. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS on ACX5448: 18.4 versions prior to 18.4R3-S10; 19.1 versions		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S8, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. **CVE ID : CVE-2022-22155**		
Improper Certificate Validation	19-Jan-22	5.8	An Improper Certificate Validation weakness in the Juniper Networks Junos OS allows an attacker to perform Person-in-the-Middle (PitM) attacks when a system script is fetched from a remote source at a specified HTTPS URL, which may compromise the integrity and confidentiality of the device. The following command can be executed by an administrator via the CLI to refresh a script from a remote location, which is affected from this vulnerability: >request system scripts refresh-from (commit | event | extension-service | op | snmp) file filename url <https-url> This issue affects: Juniper Networks Junos OS All versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to	https://kb.juniper.net/JSA11264	O-JUN-JUNO-030222/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S7; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2; 21.1 versions prior to 21.1R1-S1, 21.1R2. **CVE ID : CVE-2022-22156**		
Incorrect Authorization	19-Jan-22	5.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. JDPI incorrectly classifies out-of-state asymmetric TCP flows as the dynamic-application INCONCLUSIVE instead of UNKNOWN, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S6; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions	https://kb.juniper.net/JSA11265	O-JUN-JUNO-030222/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R2-S5, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R3-S1; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2-S1, 20.4R3; 21.1 versions prior to 21.1R1-S1, 21.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22157**		
Uncontrolled Resource Consumption	19-Jan-22	5	A vulnerability in the NETISR network queue functionality of Juniper Networks Junos OS kernel allows an attacker to cause a Denial of Service (DoS) by sending crafted genuine packets to a device. During an attack, the routing protocol daemon (rpd) CPU may reach 100% utilization, yet FPC CPUs forwarding traffic will operate normally. This attack occurs when the attackers' packets are sent over an IPv4 unicast routing equal-cost multi-path (ECMP) unilist selection. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. An indicator of compromise may be to monitor NETISR drops in the network with the assistance of JTAC. Please contact JTAC for technical support for	https://kb.juniper.net/JSA11267	O-JUN-JUNO-030222/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			further guidance. This issue affects: Juniper Networks Junos OS 17.3 version 17.3R3-S9 and later versions prior to 17.3R3-S12; 17.4 version 17.4R3-S3 and later versions prior to 17.4R3-S5; 18.1 version 18.1R3-S11 and later versions prior to 18.1R3-S13; 18.2 version 18.2R3-S6 and later versions; 18.3 version 18.3R3-S4 and later versions prior to 18.3R3-S5; 18.4 version 18.4R3-S5 and later versions prior to 18.4R3-S9; 19.1 version 19.1R3-S3 and later versions prior to 19.1R3-S7. This issue does not affect Juniper Networks Junos OS versions prior to 17.3R3-S9. This issue does not affect Juniper Networks Junos OS Evolved. **CVE ID : CVE-2022-22159**		
Unchecked Error Condition	19-Jan-22	2.9	An Unchecked Error Condition vulnerability in the subscriber management daemon (smgd) of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to cause a crash of and thereby a Denial of Service (DoS). In a subscriber management / broadband edge environment if a single session group configuration contains dual-stack and a pp0 interface, smgd will crash and restart every time a PPPoE	https://kb.juniper.net/JSA11268	O-JUN-JUNO-030222/832

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client sends a specific message. This issue affects Juniper Networks Junos OS on MX Series: 16.1 version 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1. **CVE ID : CVE-2022-22160**		
Uncontrolled Resource Consumption	19-Jan-22	5	An Uncontrolled Resource Consumption vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated network based attacker to cause 100% CPU load and the device to become unresponsive by sending a flood of traffic to the out-of-band management ethernet port. Continued receipted of a flood will create a sustained Denial of Service (DoS) condition. Once the flood subsides the system will recover by itself. An indication that the system is	https://kb.juniper.net/JSA11269	O-JUN-JUNO-030222/833

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected by this issue would be that an irq handled by the fman process is shown to be using a high percentage of CPU cycles like in the following example output: user@host> show system processes extensive ... PID USERNAME PRI NICE SIZE RES STATE TIME WCPU COMMAND 31 root -84 -187 0K 16K WAIT 22.2H 56939.26% irq96: fman0 This issue affects Juniper Networks Junos OS: All versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S4; 19.4 versions prior to 19.4R2-S5, 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2; 21.2 versions prior to 21.2R1-S1, 21.2R2. **CVE ID : CVE-2022-22161**		
Generation of Error Message Containing Sensitive Information	19-Jan-22	6.9	A Generation of Error Message Containing Sensitive Information vulnerability in the CLI of Juniper Networks Junos OS allows a locally authenticated attacker with	https://kb.juniper.net/JSA11270	O-JUN-JUNO-030222/834

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			low privileges to elevate these to the level of any other user logged in via J-Web at this time, potential leading to a full compromise of the device. This issue affects Juniper Networks Junos OS: All versions prior to 15.1R7-S11; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2. **CVE ID : CVE-2022-22162**		
Improper Input Validation	19-Jan-22	2.9	An Improper Input Validation vulnerability in the Juniper DHCP daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent unauthenticated attacker to cause a crash of jdhcpd and thereby a Denial of Service (DoS). If a device is configured as DHCPv6 local server and persistent storage is enabled, jdhcpd will crash when receiving a specific	https://kb.juniper.net/JSA11271	O-JUN-JUNO-030222/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DHCPv6 message. This issue affects: Juniper Networks Junos OS All versions prior to 15.1R7-S11; 18.4 versions prior to 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2; 21.2 versions prior to 21.2R2. **CVE ID : CVE-2022-22163**		
Improper Input Validation	19-Jan-22	3.3	An Improper Validation of Specified Quantity in Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS allows an unauthenticated networked attacker to cause an rdp crash and thereby a Denial of Service (DoS). If a BGP update message is received over an established BGP session where a BGP SR-TE policy tunnel attribute is malformed and BGP update tracing flag is enabled, the rpd will core. This issue can happen with any BGP session as long as the previous conditions are met. This issue can not propagate as the crash occurs as soon as the malformed update is	https://kb.juniper.net/JSA11274	O-JUN-JUNO-030222/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			received. This issue affects Juniper Networks Junos OS: 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22166**		
Incorrect Authorization	19-Jan-22	6.8	A traffic classification vulnerability in Juniper Networks Junos OS on the SRX Series Services Gateways may allow an attacker to bypass Juniper Deep Packet Inspection (JDPI) rules and access unauthorized networks or resources, when 'no-syn-check' is enabled on the device. While JDPI correctly classifies out-of-state asymmetric TCP flows as the dynamic-application UNKNOWN, this classification is not provided to the policy module properly and hence traffic continues to use the pre-id-default-policy, which is more permissive, causing the firewall to allow traffic to be forwarded that should have been denied. This issue only occurs when 'set security flow tcp-session no-syn-check' is configured on the device. This issue affects Juniper Networks Junos OS on SRX Series: 18.4 versions prior to 18.4R2-S10, 18.4R3-S10; 19.1 versions prior to	https://kb.juniper.net/JSA11265	O-JUN-JUNO-030222/837

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S8; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. **CVE ID : CVE-2022-22167**		
Missing Release of Memory after Effective Lifetime	19-Jan-22	6.1	An Improper Validation of Specified Type of Input vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to trigger a Missing Release of Memory after Effective Lifetime vulnerability. Continued exploitation of this vulnerability will eventually lead to an FPC reboot and thereby a Denial of Service (DoS). This issue affects: Juniper Networks Junos OS on vMX and MX150: All versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S5, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3;	https://kb.juniper.net/JSA11275	O-JUN-JUNO-030222/838

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. **CVE ID : CVE-2022-22168**		
Missing Release of Resource after Effective Lifetime	19-Jan-22	5	A Missing Release of Resource after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated networked attacker to cause a Denial of Service (DoS) by sending specific packets over VXLAN which cause heap memory to leak and on exhaustion the PFE to reset. The heap memory utilization can be monitored with the command: user@host> show chassis fpc This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R2-S6, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. This issue does not affect versions of Junos OS prior to 19.4R1. **CVE ID : CVE-2022-22170**	https://kb.juniper.net/JSA11277	O-JUN-JUNO-030222/839
Improper	19-Jan-22	5	An Improper Check for	https://kb.ju	O-JUN-JUNO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check for Unusual or Exceptional Conditions			Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated networked attacker to cause a Denial of Service (DoS) by sending specific packets over VXLAN which cause the PFE to reset. This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R3-S7; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect versions of Junos OS prior to 19.4R1. **CVE ID : CVE-2022-22171**	niper.net/JSA11277	030222/840
Improper Locking	19-Jan-22	4.3	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series and SRX Series allows an unauthenticated networked attacker to cause a flowprocessing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can occur in a scenario where the	https://kb.juniper.net/JSA11281	O-JUN-JUNO-030222/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIP ALG is enabled and specific SIP messages are being processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22175**		
Improper Input Validation	19-Jan-22	2.9	An Improper Validation of Syntactic Correctness of Input vulnerability in the Juniper DHCP daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent unauthenticated attacker sending a malformed DHCP packet to cause a crash of jdhcpd and thereby a Denial of Service (DoS). If option-82 is configured in a DHCP snooping / -security scenario, jdhcpd crashes if a specific malformed DHCP request packet is received. The DHCP functionality is impacted while jdhcpd restarts, and continued exploitation of the vulnerability will lead to the unavailability of the DHCP service and thereby a sustained DoS. This issue affects Juniper Networks	https://kb.juniper.net/JSA11282	O-JUN-JUNO-030222/842

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS 13.2 version 13.2R1 and later versions prior to 15.1R7-S11; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R2-S7, 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S3; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2. This issue does not affect Juniper Networks Junos OS version 12.3R12 and prior versions. **CVE ID : CVE-2022-22176**		
Improper Handling of Exceptional Conditions	19-Jan-22	5	A release of illegal memory vulnerability in the snmpd daemon of Juniper Networks Junos OS, Junos OS Evolved allows an attacker to halt the snmpd daemon causing a sustained Denial of Service (DoS) to the service until it is manually restarted. This issue impacts any version of SNMP – v1,v2, v3 This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S20; 15.1 versions prior to 15.1R7-S11; 18.3 versions prior to	https://kb.juniper.net/JSA11283, https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/ref/statement/client-list-edit-snmp.html	O-JUN-JUNO-030222/843

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R2-S5, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2. Juniper Networks Junos OS Evolved 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22177**		
Stack-based Buffer Overflow	19-Jan-22	5	A Stack-based Buffer Overflow vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on MX Series and SRX series allows an unauthenticated networked attacker to cause a flowd crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue can be triggered by a specific Session Initiation Protocol (SIP) invite packet if the SIP ALG is enabled. Due to this, the PIC will be rebooted	https://kb.juniper.net/JSA11284	O-JUN-JUNO-030222/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and all traffic that traverses the PIC will be dropped. This issue affects: Juniper Networks Junos OS 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R2; 21.3 versions prior to 21.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. **CVE ID : CVE-2022-22178**		
Improper Input Validation	19-Jan-22	2.9	A Improper Validation of Specified Index, Position, or Offset in Input vulnerability in the Juniper DHCP daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent unauthenticated attacker to cause a crash of jdhcpd and thereby a Denial of Service (DoS). In a scenario where DHCP relay or local server is configured the problem can be triggered if a DHCPv4 packet with specific options is received leading to a corruption of the options read from the packet. This corruption can then lead to jdhcpd crash and restart. This issue affects: Juniper Networks Junos OS 17.4R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4	https://kb.juniper.net/JSA11285	O-JUN-JUNO-030222/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2, 21.2R3; 21.3 versions prior to 21.3R1-S1, 21.3R2. **CVE ID : CVE-2022-22179**		
junos_os_evolved					
Improper Initialization	19-Jan-22	5	An Improper Initialization vulnerability in Juniper Networks Junos OS Evolved may cause a commit operation for disabling the telnet service to not take effect as expected, resulting in the telnet service staying enabled. When it is not intended to be operating on the device, an administrator can issue the following command to verify whether telnet is operating in the background: user@device > show system connections | grep :23 tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN 20879/xinetd This issue affects: Juniper Networks Junos OS Evolved All versions prior to 20.4R2-S2-EVO; 21.1 version 21.1R1-EVO and later versions; 21.2 versions prior to 21.2R2-EVO. **CVE ID : CVE-2022-22164**	https://kb.juniper.net/JSA11272	O-JUN-JUNO-030222/846

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	19-Jan-22	5	A release of illegal memory vulnerability in the snmpd daemon of Juniper Networks Junos OS, Junos OS Evolved allows an attacker to halt the snmpd daemon causing a sustained Denial of Service (DoS) to the service until it is manually restarted. This issue impacts any version of SNMP – v1,v2, v3 This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S20; 15.1 versions prior to 15.1R7-S11; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R2-S5, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S2, 21.1R3; 21.2 versions prior to 21.2R1-S2, 21.2R2. Juniper Networks Junos OS Evolved 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO. **CVE ID : CVE-2022-22177**	https://kb.juniper.net/JSA11283, https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/ref/statement/client-list-edit-snmp.html	O-JUN-JUNO-030222/847
mx150					
Missing	19-Jan-22	6.1	An Improper Validation of	https://kb.ju	O-JUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release of Memory after Effective Lifetime			Specified Type of Input vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to trigger a Missing Release of Memory after Effective Lifetime vulnerability. Continued exploitation of this vulnerability will eventually lead to an FPC reboot and thereby a Denial of Service (DoS). This issue affects: Juniper Networks Junos OS on vMX and MX150: All versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S5, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. **CVE ID : CVE-2022-22168**	niper.net/JSA11275	MX15-030222/848
vmx					
Missing Release of Memory after Effective Lifetime	19-Jan-22	6.1	An Improper Validation of Specified Type of Input vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated adjacent attacker to trigger a Missing Release of Memory after Effective Lifetime	https://kb.juniper.net/JSA11275	O-JUN-VMX-030222/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Continued exploitation of this vulnerability will eventually lead to an FPC reboot and thereby a Denial of Service (DoS). This issue affects: Juniper Networks Junos OS on vMX and MX150: All versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S5, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2; 21.3 versions prior to 21.3R1-S1, 21.3R2. **CVE ID : CVE-2022-22168**		
kingjim					
mirupass_pw10_firmware					
Missing Encryption of Sensitive Data	17-Jan-22	2.1	Missing encryption of sensitive data vulnerability in 'MIRUPASS' PW10 firmware all versions and 'MIRUPASS' PW20 firmware all versions allows an attacker who can physically access the device to obtain the stored passwords. **CVE ID : CVE-2022-0183**	https://www.kingjim.co.jp/download/security/#mirupass	O-KIN-MIRU-030222/850
mirupass_pw20_firmware					
Missing Encryption	17-Jan-22	2.1	Missing encryption of sensitive data vulnerability in	https://www.kingjim.co.	O-KIN-MIRU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			'MIRUPASS' PW10 firmware all versions and 'MIRUPASS' PW20 firmware all versions allows an attacker who can physically access the device to obtain the stored passwords. **CVE ID : CVE-2022-0183**	jp/download/security/#mirupass	030222/851
spc10_firmware					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	https://www.kingjim.co.jp/download/security/#sr01	O-KIN-SPC1-030222/852
tepura_pro_sr-7900p_firmware					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	https://www.kingjim.co.jp/download/security/#sr01	O-KIN-TEPU-030222/853
tepura_pro_sr5900p_firmware					
Insufficiently Protected Credentials	17-Jan-22	3.3	Insufficiently protected credentials vulnerability in 'TEPRA' PRO SR5900P	https://www.kingjim.co.jp/download	O-KIN-TEPU-030222/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ver.1.080 and earlier and 'TEPRA' PRO SR-R7900P Ver.1.030 and earlier allows an attacker on the adjacent network to obtain credentials for connecting to the Wi-Fi access point with the infrastructure mode. **CVE ID : CVE-2022-0184**	/security/#sr01	
Linux					
linux_kernel					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-LIN-LINU-030222/855
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jan-22	4.3	A directory traversal vulnerability in Trend Micro Deep Security and Cloud One - Workload Security Agent for Linux version 20 and below could allow an attacker to read arbitrary files from the file system. Please note: an attacker must first obtain compromised access to the target Deep Security Manager (DSM) or the target agent must be not yet activated or configured in order to exploit this vulnerability. **CVE ID : CVE-2022-23119**	https://success.trendmicro.com/solution/000290104	O-LIN-LINU-030222/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	20-Jan-22	6.9	A code injection vulnerability in Trend Micro Deep Security and Cloud One - Workload Security Agent for Linux version 20 and below could allow an attacker to escalate privileges and run arbitrary code in the context of root. Please note: an attacker must first obtain access to the target agent in an un-activated and unconfigured state in order to exploit this vulnerability. **CVE ID : CVE-2022-23120**	https://success.trendmicro.com/solution/000290104	O-LIN-LINU-030222/857
Microsoft					
windows					
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-MIC-WIND-030222/858
Insertion of Sensitive Information into Log File	17-Jan-22	2.1	In Stormshield SSO Agent 2.x before 2.1.1 and 3.x before 3.0.2, the cleartext user password and PSK are contained in the log file of the .exe installer. **CVE ID : CVE-2022-22703**	https://advisories.stormshield.eu/2022-001	O-MIC-WIND-030222/859
Oracle					
solaris					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-22	6	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Fault Management Architecture). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. 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 Oracle Solaris accessible data as well as unauthorized read access to a subset of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L). **CVE ID : CVE-2022-21263**	https://www.oracle.com/security-alerts/cpujan2022.html	O-ORA-SOLA-030222/860
N/A	19-Jan-22	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Install). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged	https://www.oracle.com/security-alerts/cpujan2022.html	O-ORA-SOLA-030222/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. 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 Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2022-21298**		
N/A	19-Jan-22	4.9	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5	https://www.oracle.com/security-alerts/cpujan2022.html	O-ORA-SOLA-030222/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2022-21375**		
Use of a Broken or Risky Cryptographic Algorithm	19-Jan-22	6.4	IBM WebSphere Application Server Liberty 21.0.0.10 through 21.0.0.12 could provide weaker than expected security. A remote attacker could exploit this weakness to obtain sensitive information and gain unauthorized access to JAX-WS applications. IBM X-Force ID: 217224. **CVE ID : CVE-2022-22310**	https://exchange.xforce.ibmcloud.com/vulnerabilities/217224, https://www.ibm.com/support/pages/node/6541530	O-ORA-SOLA-030222/863