



# CVE-2021-2024

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-2024   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert_us@oracle.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2021-01-20 15:15:00 UTC   |
| <b>Updated</b>         | 2022-01-04 17:27:00 UTC   |
| <b>Description</b>     | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are a |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                                       | Version | Update | Edition | Language |
|-------------|------------------------|---|---------|--------|---------|----------|
| Application | <a href="#">Netapp</a> | <a href="#">Oncommand Insight</a>             | -       | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Oncommand Insight</a>             | -       | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Oncommand Workflow Automation</a> | -       | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Oncommand Workflow Automation</a> | -       | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Snapcenter</a>                    | -       | All    | All     | All      |
| Application | <a href="#">Netapp</a> | <a href="#">Snapcenter</a>                    | -       | All    | All     | All      |
| Application | <a href="#">Oracle</a> | <a href="#">Mysql</a>                         | All     | All    | All     | All      |

## References

| Reference   | Source  | Link                                | Tags                |
|---|---------|-------------------------------------|---------------------|
| MySQL: Multiple vulnerabilities (GLSA 202105-27) — Gentoo security              | GENTOO  | <a href="#">security.gentoo.org</a> |                     |
| January 2021 MySQL Vulnerabilities in NetApp Products   NetApp Product Security | CONFIRM | <a href="#">security.netapp.com</a> | Third Party Advisor |
| Oracle Critical Patch Update Advisory - January 2021                            | MISC    | <a href="#">www.oracle.com</a>      | Vendor Advisory     |
| CVE Program record  | CVE.ORG | <a href="#">www.cve.org</a>         | canonical           |
| NVD vulnerability detail  | NVD     | <a href="#">nvd.nist.gov</a>        | canonical, analysis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159407 Oracle Enterprise Linux Security Update for mysql:8.0 (ELSA-2021-3590)

239646 Red Hat Update for mysql:8.0 (RHSA-2021:3590)

239672 Red Hat Update for rh-mysql80-mysql (RHSA-2021:3811)

690266 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (31344707-5d87-11eb-929d-d4c9ef517024)

710088 Gentoo Linux MySQL Multiple vulnerabilities (GLSA 202105-27)

900182 CBL-Mariner Linux Security Update for mysql 8.0.22

903626 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (3781)

940376 AlmaLinux Security Update for mysql:8.0 (ALSA-2021:3590)

960033 Rocky Linux Security Update for mysql:8.0 (RLSA-2021:3590)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)