



# CVE-2020-14591

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2020-14591   |
| <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>       | 2020-07-15 18:15:00 UTC  |
| <b>Updated</b>         | 2022-09-30 03:23:00 UTC  |
| <b>Description</b>     | Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that ar |

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                                       | Version | Update | Edition | Language |
|------------------|-------------------------------|---|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>                        | 31      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>                        | 32      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>                        | 33      | All    | All     | All      |
| Application      | <a href="#">Netapp</a>        | <a href="#">Active Iq Unified Manager</a>     | -       | All    | All     | All      |
| Application      | <a href="#">Netapp</a>        | <a href="#">Active Iq Unified Manager</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="#">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> |                        |
| July 2020 MySQL Vulnerabilities in NetApp Products   NetApp Product Security | CONFIRM | <a href="#">security.netapp.com</a> | Third Party Advisory   |
| Oracle Critical Patch Update Advisory - July 2020                            | MISC    | <a href="#">www.oracle.com</a>      | Patch, Vendor Advisory |
| USN-4441-1: MySQL vulnerabilities   Ubuntu security notices   Ubuntu         | UBUNTU  | <a href="#">usn.ubuntu.com</a>      |                        |
| CVE Program record   | CVE.ORG | <a href="#">www.cve.org</a>         | canonical              |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

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

[900192](#) CBL-Mariner Linux Security Update for mysql 8.0.20

[903330](#) Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (1862)

© [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](#)