# CVE-2020-2924

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-2924 |
| **State** | PUBLIC |
| **Assigner** | secalert_us@oracle.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-04-15 14:15:00 UTC |
| **Updated** | 2023-11-07 03:21:00 UTC |
| **Description** | 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 |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 20.04 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Fedoraproject | Fedora | 31 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Application | Netapp | Active Iq Unified Manager | All | All | All | All |
| Application | Netapp | Active Iq Unified Manager | All | All | All | All |
| Application | Netapp | Oncommand Insight | - | All | All | All |
| Application | Netapp | Oncommand Workflow Automation | - | All | All | All |
| Application | Netapp | Snapcenter | - | All | All | All |
| Application | Oracle | Mysql | All | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| [SECURITY] Fedora 31 Update: community-mysql-8.0.20-1.fc31 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |

| | | |
|---|---|---|
| MySQL: Multiple vulnerabilities (GLSA 202105-27) — Gentoo security | GENTOO | security.gentoo.or |
| [SECURITY] Fedora 32 Update: community-mysql-8.0.20-1.fc32 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |
| USN-4350-1: MySQL vulnerabilities \| Ubuntu security notices | UBUNTU | usn.ubuntu.com |
| [SECURITY] Fedora 30 Update: community-mysql-8.0.20-1.fc30 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| Oracle Critical Patch Update Advisory - April 2020 | MISC | www.oracle.com |
| [SECURITY] Fedora 30 Update: community-mysql-8.0.20-1.fc30 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject |
| April 2020 MySQL Vulnerabilities in NetApp Products \| NetApp Product Security | CONFIRM | security.netapp.cc |
| [SECURITY] Fedora 32 Update: community-mysql-8.0.20-1.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| [SECURITY] Fedora 31 Update: community-mysql-8.0.20-1.fc31 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

940103 AlmaLinux Security Update for mysql:8.0 (ALSA-2020:3732)

960190 Rocky Linux Security Update for mysql:8.0 (RLSA-2020:3732)

© 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 registred 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.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**