



# CVE-2019-2537

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-2537
<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>	2019-01-16 19:30:00 UTC
<b>Updated</b>	2022-08-15 14:29:00 UTC
<b>Description</b>	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are

## 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="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Mariadb</a>	<a href="#">Mariadb</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Unified Manager</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Unified Manager</a>	All	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	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.6	All	All	All

## References

Reference	Source	Link	Tags
January 2019 MySQL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party Advi
MariaDB, MySQL: Multiple vulnerabilities (GLSA 201908-24) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
USN-3867-1: MySQL vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advi
[SECURITY] [DLA 1655-1] mariadb-10.0 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Third Party Advi
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Malformed Request	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advi
Oracle Critical Patch Update - January 2019	CONFIRM	<a href="https://www.oracle.com">www.oracle.com</a>	Patch, Vendor A
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analy

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159650 Oracle Enterprise Linux Security Update for mariadb:10.3 security and bug fix update (ELSA-2019-3708)

<a href="#">377107</a> Alibaba Cloud Linux Security Update for mysql:8.0 (ALINUX3-SA-2022:0107)
<a href="#">377122</a> Alibaba Cloud Linux Security Update for mariadb:10.3 and mariadb-devel:10.3 (ALINUX3-SA-2021:0030)
<a href="#">500378</a> Alpine Linux Security Update for mariadb
<a href="#">504136</a> Alpine Linux Security Update for mariadb
<a href="#">710137</a> Gentoo Linux MariaDB, MySQL Multiple vulnerabilities (GLSA 201908-24)
<a href="#">940079</a> AlmaLinux Security Update for mysql:8.0 (ALSA-2019:2511)
<a href="#">940341</a> AlmaLinux Security Update for mariadb:10.3 (ALSA-2019:3708)
<a href="#">960793</a> Rocky Linux Security Update for mysql:8.0 (RLSA-2019:2511)

© [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](#)**