



# CVE-2022-24052

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

## Summary

<b>CVE</b>	CVE-2022-24052
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-18 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:44:00 UTC
<b>Description</b>	MariaDB CONNECT Storage Engine Heap-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allow

## Risk And Classification

**Problem Types:** CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Mariadb</a>	<a href="#">Mariadb</a>	All	All	All	All
Application	<a href="#">Mariadb</a>	<a href="#">Mariadb</a>	10.8.0	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 34 Update: mariadb-10.5.15-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
ZDI-22-367   Zero Day Initiative	MISC	<a href="#">www.zerodayinitiative.com</a>
[SECURITY] Fedora 35 Update: mariadb-10.5.15-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: galera-26.4.11-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
February 2022 MariaDB Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
[SECURITY] Fedora 34 Update: mariadb-10.5.15-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
Security Vulnerabilities Fixed in MariaDB - MariaDB Knowledge Base	MISC	<a href="#">mariadb.com</a>
[SECURITY] Fedora 35 Update: mariadb-10.5.15-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: galera-26.4.11-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [160019](#) Oracle Enterprise Linux Security Update for mariadb:10.5 (ELSA-2022-5826)
- [160037](#) Oracle Enterprise Linux Security Update for galera, mariadb, and mysql-selinux (ELSA-2022-5948)
- [160096](#) Oracle Enterprise Linux Security Update for mariadb:10.3 (ELSA-2022-6443)
- [179218](#) Debian Security Update for mariadb-10.5mariadb-10.3 (CVE-2022-24052)
- [198679](#) Ubuntu Security Notification for MariaDB Vulnerabilities (USN-5305-1)
- [240565](#) Red Hat Update for rh-mariadb105-galera and rh-mariadb105-mariadb (RHSA-2022:5759)
- [240586](#) Red Hat Update for mariadb:10.5 security (RHSA-2022:5826)
- [240596](#) Red Hat Update for galera, mariadb, and mysql-selinux security (RHSA-2022:5948)
- [240645](#) Red Hat Update for rh-mariadb103-galera and rh-mariadb103-mariadb (RHSA-2022:6306)
- [240665](#) Red Hat Update for mariadb:10.3 (RHSA-2022:6443)
- [282654](#) Fedora Security Update for galera (FEDORA-2022-03350936ee)
- [282655](#) Fedora Security Update for mariadb (FEDORA-2022-5cfe372ab7)
- [282722](#) Fedora Security Update for galera (FEDORA-2022-263f7cc483)
- [354437](#) Amazon Linux Security Advisory for mariadb105 : ALAS2022-2022-069
- [354476](#) Amazon Linux Security Advisory for mariadb105 : ALAS2022-2022-182
- [355152](#) Amazon Linux Security Advisory for mariadb105 : ALAS2023-2023-037
- [356265](#) Amazon Linux Security Advisory for mariadb : ALASMARIADB10.5-2023-003
- [376523](#) MariaDB Multiple Vulnerabilities
- [377368](#) Alibaba Cloud Linux Security Update for mariadb:10.5 (ALINUX3-SA-2022:0151)
- [500389](#) Alpine Linux Security Update for mariadb
- [501433](#) Alpine Linux Security Update for mariadb
- [501971](#) Alpine Linux Security Update for mariadb
- [502457](#) Alpine Linux Security Update for mariadb
- [504147](#) Alpine Linux Security Update for mariadb

690789 Free Berkeley Software Distribution (FreeBSD) Security Update for mariadb (ff5606f7-8a45-11ec-8be6-d4c9ef517024)
751802 SUSE Enterprise Linux Security Update for mariadb (SUSE-SU-2022:0726-1)
751805 SUSE Enterprise Linux Security Update for mariadb (SUSE-SU-2022:0725-1)
751808 OpenSUSE Security Update for mariadb (openSUSE-SU-2022:0731-1)
751811 OpenSUSE Security Update for mariadb (openSUSE-SU-2022:0725-1)
751812 OpenSUSE Security Update for mariadb (openSUSE-SU-2022:0726-1)
751841 SUSE Enterprise Linux Security Update for mariadb (SUSE-SU-2022:0782-1)
753158 SUSE Enterprise Linux Security Update for mariadb (SUSE-SU-2022:0731-1)
753364 SUSE Enterprise Linux Security Update for mariadb (SUSE-SU-2022:2561-1)
900683 Common Base Linux Mariner (CBL-Mariner) Security Update for mariadb (8685)
901770 Common Base Linux Mariner (CBL-Mariner) Security Update for mariadb (8667-1)
940606 AlmaLinux Security Update for mariadb:10.5 (ALSA-2022:5826)
940632 AlmaLinux Security Update for galera, (ALSA-2022:5948)
940668 AlmaLinux Security Update for mariadb:10.3 (ALSA-2022:6443)
960383 Rocky Linux Security Update for mariadb:10.5 (RLSA-2022:5826)
960482 Rocky Linux Security Update for galera, (RLSA-2022:5948)

© [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](#)