RHSA-2023:5684 - Security Advisory

Issued: 2023-10-12 Updated: 2023-10-12

Synopsis

Important: galera and mariadb security update

Type/Severity

Security Advisory: Important

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

An update for galera and mariadb is now available for Red Hat Enterprise Linux 9.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

Description

MariaDB is a multi-user, multi-threaded SQL database server that is binary compatible with MySQL.

The following packages have been upgraded to a later upstream version: galera (26.4.14), mariadb (10.5.22).

Security Fix(es):

- mariadb: node crashes with Transport endpoint is not connected mysqld got signal 6 (CVE-2023-5157)
- mariadb: use-after-poison in prepare_inplace_add_virtual in handler0alter.cc (CVE-2022-32081)
- mariadb: assertion failure at table->get_ref_count() == 0 in dict0dict.cc (CVE-2022-32082)
- mariadb: segmentation fault via the component sub_select (CVE-2022-32084)
- mariadb: server crash in st_select_lex_unit::exclude_level (CVE-2022-32089)
- mariadb: server crash in JOIN_CACHE::free or in copy_fields (CVE-2022-32091)
- mariadb: compress_write() fails to release mutex on failure (CVE-2022-38791)
- mariadb: NULL pointer dereference in spider_db_mbase::print_warnings() (CVE-2022-47015)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Solution

For details on how to apply this update, which includes the changes described in this advisory, refer to:

https://access.redhat.com/articles/11258

After installing this update, the MariaDB server daemon (mysqld) will be restarted automatically.

Affected Products

- Red Hat Enterprise Linux for x86_64 9 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64
- Red Hat Enterprise Linux Server - AUS 9.6 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86_64
- Red Hat Enterprise Linux for IBM z Systems 9 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for Power, little endian 9 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le

- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for ARM 64 9 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
- Red Hat CodeReady Linux Builder for x86_64 9 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 9 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64

- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x

Fixes

- BZ - 2106028 - CVE-2022-32081 mariadb: use-after-poison in prepare_inplace_add_virtual in handler0alter.cc
- BZ - 2106030 - CVE-2022-32082 mariadb: assertion failure at table->get_ref_count() == 0 in dict0dict.cc
- BZ - 2106034 - CVE-2022-32084 mariadb: segmentation fault via the component sub_select
- BZ - 2106035 - CVE-2022-32089 mariadb: server crash in st_select_lex_unit::exclude_level
- BZ - 2106042 - CVE-2022-32091 mariadb: server crash in JOIN_CACHE::free or in copy_fields
- BZ - 2130105 - CVE-2022-38791 mariadb: compress_write() fails to release mutex on failure
- BZ - 2163609 - CVE-2022-47015 mariadb: NULL pointer dereference in spider_db_mbase::print_warnings()
- BZ - 2240246 - CVE-2023-5157 mariadb: node crashes with Transport endpoint is not connected mysqld got signal 6

CVEs

- CVE-2022-32081
- CVE-2022-32082
- CVE-2022-32084
- CVE-2022-32089
- CVE-2022-32091
- CVE-2022-38791
- CVE-2022-47015
- CVE-2023-5157

References

- https://access.redhat.com/security/updates/classification/#important

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.