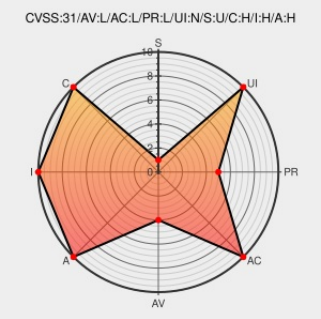
CVE-2020-7221

Published on: 02/04/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-7221

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mariadb from Mariadb contain the following vulnerability:

mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.

CVE-2020-7221 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bug 1160868 – VUL-0: CVE-2020-7221: mariadb: auth_pam_tool runtime permission setting allows	Exploit, Issue Tracking	MISC bugzilla.suse.com/show_bug.cgi?id=1160868

privilege escalation from mysql user to root	Third Party Advisory bugzilla.suse.com text/html	
oss-sec: CVE-2020-7221: mariadb: possible local mysql to root user exploit in mysql_install_db script setting permissions of /usr/lib64/mysql/plugin/auth_pam_tool_dir/auth_pam_tool	Exploit Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/oss-sec/2020/q1/55
rpm/deb and auth_pam_tool_dir/auth_pam_tool · MariaDB/server@9d18b62 · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/MariaDB/server/commit/9d18b6246755472c832

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mariadb	Mariadb	All	All	All	All

cpe:2.3:a:mariadb:mariadb:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→