



CVE-2020-28912

Published on: 12/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:27 PM UTC

CVE-2020-28912

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mariadb](#) from [Mariadb](#) contain the following vulnerability:

With MariaDB running on Windows, when local clients connect to the server over named pipes, it's possible for an unprivileged user with an ability to run code on the server machine to intercept the named pipe connection and act as a man-in-the-middle, gaining access to all the data passed between the client and the server, and getting the ability to

run SQL commands on behalf of the connected user. This occurs because of an incorrect security descriptor. This affects MariaDB Server before 10.1.48, 10.2.x before 10.2.35, 10.3.x before 10.3.26, 10.4.x before 10.4.16, and 10.5.x before 10.5.7. NOTE: this issue exists because certain details of the MariaDB CVE-2019-2503 fix did not comprehensively address attack variants against MariaDB. This situation is specific to MariaDB, and thus CVE-2020-28912 does NOT apply to other vendors that were originally affected by CVE-2019-2503.

CVE-2020-28912 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **4.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[MDEV-24040] Named pipe permission issue - Jira	Issue Tracking Vendor Advisory jira.mariadb.org text/html	MISC jira.mariadb.org/browse/MDEV-24040
HackerOne	Third Party Advisory hackerone.com text/html	h MISC hackerone.com/reports/1019891

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
Application	Mariadb	Mariadb	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
cpe:2.3:a:mariadb:mariadb:*.***.***.***:						
cpe:2.3:a:mariadb:mariadb:*.***.***.***:						
cpe:2.3:o:microsoft:windows:-.***.***.***:						
cpe:2.3:o:microsoft:windows:-.***.***.***:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

