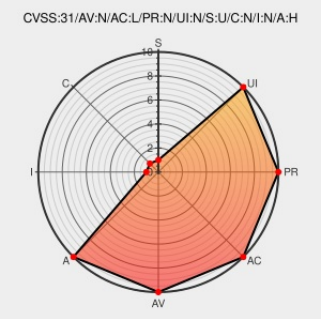
CVE-2021-3119

Published on: 03/25/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 04:04:00 PM UTC

CVE-2021-3119

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



Certain versions of Sqlcipher from Zetetic contain the following vulnerability:

Zetetic SQLCipher 4.x before 4.4.3 has a NULL pointer dereferencing issue related to sqlcipher_export in crypto.c and sqlite3StrICmp in sqlite3.c. This may allow an attacker to perform a remote denial of service attack. For example, an SQL injection can be used to execute the crafted SQL command sequence, which causes a segmentation fault.

CVE-2021-3119 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
fix sqlcipher_export handling of NULL parameters ·	github.com text/html	MISC github.com/sqlcipher/sqlcipher/commit/cb71f53e8cea4802509f182fa5bead0ac6ab0e7f#dif

sqlcipher/sqlcipher@cb71f53 · GitHub		9305215a9a0ea69300281fc4af90bc7f3437e34a0e1745d030213152993ddae4
	www.telekom.com application/pdf	MISC www.telekom.com/resource/blob/621186/3fb50ca7a4a97728be18717ed7b0062c/dl-210308-critical-dos-vulnerability-in-sqlcipher-sql-command-processing-data.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zetetic	Sqlcipher	All	All	All	All

cpe:2.3:a:zetetic:sqlcipher:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→