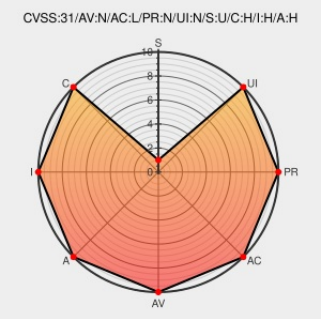
CVE-2020-26759

Published on: 01/06/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26759

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



Certain versions of Clickhouse-driver from Clickhouse-driver Project contain the following vulnerability:

clickhouse-driver before 0.1.5 allows a malicious clickhouse server to trigger a crash or execute arbitrary code (on a database client) via a crafted server response, due to a buffer overflow.

CVE-2020-26759 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Fix read_varint overflow · mymarilyn/clickhouse-driver@d708ed5 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/mymarilyn/clickhouse-driver/commit/d708ed548e1d6f254ba81a21de8ba543a53b5598

Fix malformed read/write in BufferedReader · mymarilyn/clickhouse-driver@3e99054 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mymarilyn/clickhouse-driver/commit/3e990547e064b8fca916b23a0f7d6fe8c63c7f6b

Related QID Numbers

982816 Python (pip) Security Update for clickhouse-driver (GHSA-vgv5-cxvh-vfxh)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clickhouse-driver Project	Clickhouse-driver	All	All	All	All
Application	Clickhouse-driver Project	Clickhouse-driver	All	All	All	All

cpe:2.3:a:clickhouse-driver_project:clickhouse-driver:*:*:*:*:*:*:*:*:

cpe:2.3:a:clickhouse-driver_project:clickhouse-driver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→