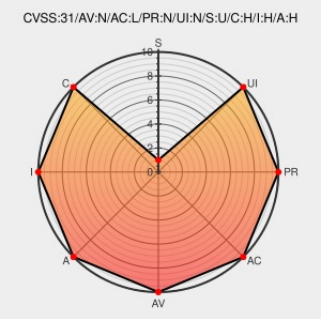
CVE-2020-17446

Published on: 08/12/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 08:37:00 PM UTC

CVE-2020-17446

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

asyncpg before 0.21.0 allows a malicious PostgreSQL server to trigger a crash or execute arbitrary code (on a database client) via a crafted server response, because of access to an uninitialized pointer in the array data decoder.

CVE-2020-17446 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
Release asyncpg v0.21.0 · MagicStack/asyncpg · GitHub	Patch, Release Notes, Third Party Advisory, github.com, text/html	CONFIRM github.com/MagicStack/asyncpg/releases/tag/v0.21.0

[SECURITY] [DLA 2363-1] asyncpg security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200902 [SECURITY] [DLA 2363-1] asyncpg security update

Related QID Numbers

982733 Python (pip) Security Update for asyncpg (GHSA-2xpj-f5g2-8p7m)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Magic	Asyncpg	All	All	All	All
Application	Magic	Asyncpg	All	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:magic:asyncpg:*:*:*:*:*:*:*:*:

cpe:2.3:a:magic:asyncpg:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→