Twisted SSH client and server denial of service during SSH handshake.

Moderate **adiroiban** published **GHSA-rv6r-3f5q-9rgx** on Mar 3

Package

twisted (pip)

Affected versions	Patched versions
> 21.7.0	22.2.0

Description

Impact

The Twisted SSH client and server implementation naively accepted an infinite amount of data for the peer's SSH version identifier.

A malicious peer can trivially craft a request that uses all available memory and crash the server, resulting in denial of service. The attack is as simple as `nc -rv localhost 22 < /dev/zero`.

Patches

The issue was fix in GitHub commit `98387b3`

A fix is available in Twisted 22.2.0.

Workarounds

- Limit access to the SSH server only to trusted source IP addresses.
- Connect over SSH only to trusted destination IP addresses.

References

Reported at https://twistedmatrix.com/trac/ticket/10284
Discussions at GHSA-rv6r-3f5q-9rgx

For more information

Found by vin01

Severity

Moderate

CVE ID

CVE-2022-21716

Weaknesses

No CWEs

Credits

 Idan-D

 vin01