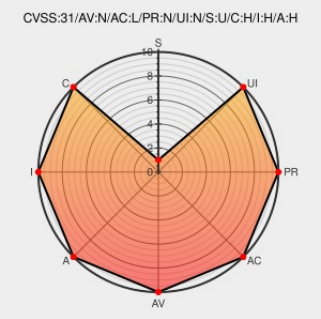
CVE-2022-29077

Published on: Not Yet Published

Last Modified on: 05/04/2022 03:41:00 PM UTC

CVE-2022-29077

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



Certain versions of Rippled from Ripple contain the following vulnerability:

A heap-based buffer overflow exists in rippled before 1.8.5. The vulnerability allows attackers to cause a crash or execute commands remotely on a rippled node, which may lead to XRPL mainnet DoS or compromise. This exposes all digital assets on the XRPL to a security threat.

CVE-2022-29077 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
Global Payment Solutions - Instant Processing | Ripple	ripple.com text/html	MISC ripple.com/
Comparing 1.8.4...1.8.5 · ripple/rippled · GitHub	github.com	MISC github.com/ripple/rippled/compare/1.8.4...1.8.5

Comparing 1.8.4...1.8.5 · ripple/rippled · GitHub	text/html	MISC github.com/ripple/rippled/compare/1.8.4...1.8.5
Introducing XRP Ledger version 1.8.5 - XRP Ledger Blog	xrpl.org text/html	{x} MISC xrpl.org/blog/2022/rippled-1.8.5.html

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	Ripple	Rippled	All	All	All	All

cpe:2.3:a:ripple:rippled:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29077 : A heap-based buffer overflow exists in rippled before 1.8.5. The vulnerability allows attackers to… twitter.com/i/web/status/1…	2022-04-25 03:08:04
/r/netcve	CVE-2022-29077	2022-04-25 03:39:12

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report