



CVE-2019-16762

Published on: 11/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:48 PM UTC

CVE-2019-16762 - advisory for cve/GHSA-425c-ccf3-3jrr

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:H



Certain versions of [Slpjs](#) from [Simpleledger](#) contain the following vulnerability:

A specially crafted Bitcoin script can cause a discrepancy between the specified SLP consensus rules and the validation result of the slpjs npm package. An attacker could create a specially crafted Bitcoin script in order to cause a hard-fork from the SLP consensus. Affected users can upgrade to any version $\geq 0.21.4$.

CVE-2019-16762 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [simpleledger](#) - [slpjs](#) version $< 0.21.4$

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Validator parsing discrepancy due to string encoding · Advisory · simpleledger/slpjs · GitHub

Exploit

Patch

Third Party Advisory

github.com

text/html

CONFIRM github.com/simpleledger/slpjs/security/advisories/GHSA-425c-ccf3-3jrr

0.21.4 updates: · simpleledger/slpjs@ac8809b · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC github.com/simpleledger/slpjs/commit/ac8809b42e47790a6f0205991b36f2699ed10c84#fe58606994c412ba56a65141a7aa4a62L701

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.

Related QID Numbers

983141 Nodejs (npm) Security Update for slpjs (GHSA-425c-ccf3-3jrr)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Simpleledger	Slpjs	All	All	All	All
Application	Simpleledger	Slpjs	All	All	All	All
cpe:2.3:a:simpleledger:slpjs:*:*:*:*:node.js:*:*:						
cpe:2.3:a:simpleledger:slpjs:*:*:*:*:node.js:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →