



CVE-2019-16761

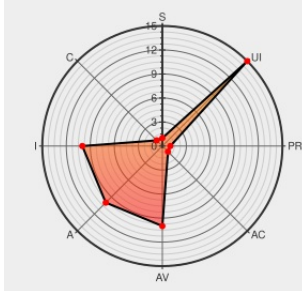
Published on: 11/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16761 - advisory for GHSA-wmx6-vxcf-c3gr

[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 [Slp-validate](#) 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 slp-validate@1.0.0 npm package. An attacker could create a specially crafted Bitcoin script in order to cause a hard-fork from the SLP consensus. All versions >1.0.0 have been patched.

CVE-2019-16761 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: simpleledger - slp-validate version = 1.0.0

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
-------------	------	------

1.0.1 updates: · simpleledger/slp-validate.js@50ad96c · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/simpleledger/slp-validate/commit/50ad96c2798dad6b9f9a13333dd05232defe5730#diff-fe58606994c412ba56a65141a7aa4a62L123

Validator parsing discrepancy due to string encoding · Advisory · simpleledger/slp-validate.js · GitHub

Patch

Third Party Advisory

github.com

text/html

CONFIRM

github.com/simpleledger/slp-validate/security/advisories/GHSA-wmx6-vxcf-c3gr

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

983868 Nodejs (npm) Security Update for slp-validate (GHSA-wmx6-vxcf-c3gr)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Simpleledger	Slp-validate	1.0.0	All	All	All
Application	Simpleledger	Slp-validate	1.0.0	All	All	All
cpe:2.3:a:simpleledger:slp-validate:1.0.0:*****:						
cpe:2.3:a:simpleledger:slp-validate:1.0.0:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →