



CVE-2020-15131

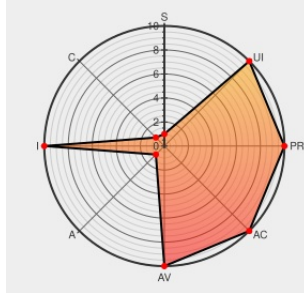
Published on: 07/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15131 - advisory for GHSA-6jmr-jfh7-xg3h

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

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



Certain versions of [Slp-validate](#) from [Simpleledger](#) contain the following vulnerability:

In SLP Validate (npm package slp-validate) before version 1.2.2, there is a vulnerability to false-positive validation outcomes for the NFT1 Child Genesis transaction type. A poorly implemented SLP wallet or opportunistic attacker could create a seemingly valid NFT1 child token without burning any of the NFT1 Group token type as is required by the NFT1 specification. This is fixed in version 1.2.2.

CVE-2020-15131 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: simpleledger - slp-validate.js version < 1.2.2

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

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

False-positive validity for NFT1 genesis transactions · Advisory · simpleledger/slp-validate.js · GitHub

Third Party Advisory

github.com

text/html

 CONFIRM github.com/simpleledger/slp-validate.js/security/advisories/GHSA-6jmr-jfh7-xg3h

critical update for NFT child genesis validation · simpleledger/slp-validate.js@3963cf9 · GitHub

Patch

Third Party Advisory

github.com

text/html

 MISC github.com/simpleledger/slp-validate.js/commit/3963cf914afae69084059b82483da916d97af65c

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

983862 Nodejs (npm) Security Update for slp-validate (GHSA-6jmr-jfh7-xg3h)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simpleledger	Slp-validate	All	All	All	All
Application	Simpleledger	Slp-validate	All	All	All	All
cpe:2.3:a:simpleledger:slp-validate:*****:.*						
cpe:2.3:a:simpleledger:slp-validate:*****:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)