



CVE-2020-11071

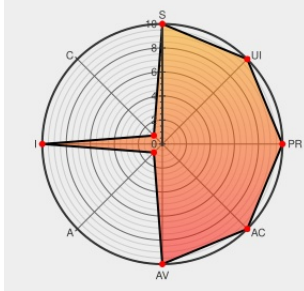
Published on: 05/11/2020 12:00:00 AM UTC

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

CVE-2020-11071 - advisory for GHSA-jc83-cpf9-q7c6

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

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



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

SLPJS (npm package slpjs) before version 0.27.2, has a vulnerability where users could experience false-negative validation outcomes for MINT transaction operations. A poorly implemented SLP wallet could allow spending of the affected tokens which would result in the destruction of a user's minting baton. This is fixed in version 0.27.2.

CVE-2020-11071 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [simpleledger](#) - [slpjs](#) version < 0.27.2

CVSS3 Score: **8.6 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	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-negative validation results	Tool Signature	CONFIRM github.com/simpleledger/slpjs/security/advisories/GHSA-jc83-cpf9-q7c6

in MINT transactions with invalid baton · Advisory · simpleledger/slpjs · GitHub

github.com

text/html

fix false negative case for MINT transactions · simpleledger/slpjs@3671be2 · GitHub

Patch

Tool Signature

github.com

text/html

MISC

github.com/simpleledger/slpjs/commit/3671be2ffb6d4cfa94c00c6dc8649d1ba1d75754

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

983130 Nodejs (npm) Security Update for slpjs (GHSA-jc83-cpf9-q7c6)

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