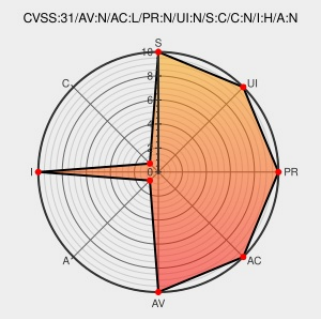
CVE-2020-11072

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

Last Modified on: 03/23/2021 11:23:25 PM UTC

CVE-2020-11072 - advisory for GHSA-4w97-57v2-3w44

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



Certain versions of Slp-validate from Simpleledger contain the following vulnerability:

In SLP Validate (npm package slp-validate) before version 1.2.1, 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 has been fixed in slp-validate in version 1.2.1. Additonally, slpjs version 0.27.2 has a related fix under related CVE-2020-11071.

CVE-2020-11072 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **simpleledger** - **slp-validate** version **< 1.2.1**

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

fix false negative case for MINT transactions · simpleledger/slp-validate.js@cde95c0 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/simpleledger/slp-validate/commit/cde95c0c6470dceb4f023cd462f904135ebd73e7
False-negative validation results in MINT transactions with invalid baton · Advisory · simpleledger/slp-validate.js · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/simpleledger/slp-validate/security/advisories/GHSA-4w97-57v2-3w44

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

983866 Nodejs (npm) Security Update for slp-validate (GHSA-4w97-57v2-3w44)

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→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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