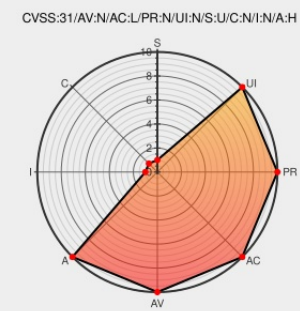
CVE-2023-36198

Published on: Not Yet Published

Last Modified on: 08/29/2023 08:53:00 PM UTC

CVE-2023-36198

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



Certain versions of Sgxwallet from Skale contain the following vulnerability:

Buffer Overflow vulnerability in skalenetwork sgxwallet v.1.9.0 allows an attacker to cause a denial of service via the trustedBlsSignMessage function.

CVE-2023-36198 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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	NONE	HIGH

CVE References

Description	Tags	Link
Two bugs on SGXWallet · Issue #419 · skalenetwork/sgxwallet · GitHub	github.com text/html	MISC github.com/skalenetwork/sgxwallet/issues/419

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Skale	Sgxwallet	1.9.0	All	All	All

cpe:2.3:a:skale:sgxwallet:1.9.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→