

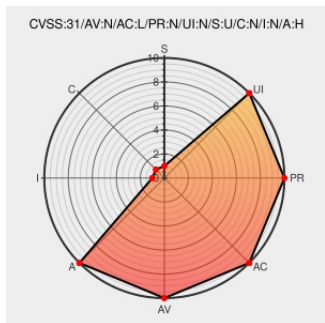


CVE-2021-36218

Published on: 09/27/2021 12:00:00 AM UTC

Last Modified on: 10/02/2021 02:05:00 AM UTC

CVE-2021-36218

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

Certain versions of [Sgxwallet](#) from [Skale](#) contain the following vulnerability:

An issue was discovered in SKALE sgxwallet 1.58.3. `sgx_disp_ippsAES_GCMEncrypt` allows an out-of-bounds write, resulting in a segfault and compromised enclave. This issue describes a buffer overflow, which was resolved prior to v1.77.0 and not reproducible in latest sgxwallet v1.77.0

CVE-2021-36218 has been assigned by [M](#) 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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Releases · skalenetwork/sgxwallet · GitHub	github.com text/html	MISC github.com/skalenetwork/sgxwallet/releases
SKAI F-3205-restart ·	github.com	MISC

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	1.58.3	All	All	All
cpe:2.3:a:skale:sgxwallet:1.58.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-36218 : An issue was discovered in SKALE sgxwallet 1.58.3. sgx_disp_ippsAES_GCMEncrypt allows an out-of-bo... twitter.com/i/web/status/1...	2021-09-27 14:07:08
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-36218 Description: CVE-2021-36218 An issue was discovered in SKALE sgxw... twitter.com/i/web/status/1...	2021-09-27 15:00:04

← Previous ID

Next ID→