



CVE-2023-33241

Published on: Not Yet Published

Last Modified on: 08/25/2023 04:14:00 PM UTC

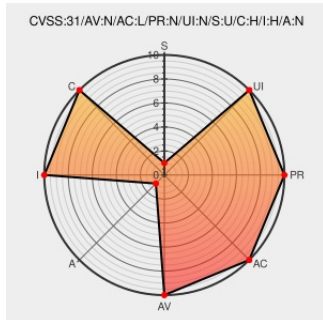
CVE-2023-33241

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Gg18](#) from [Gg18 Project](#) contain the following vulnerability:

Crypto wallets implementing the GG18 or GG20 TSS protocol might allow an attacker to extract a full ECDSA private key by injecting a malicious pallier key and cheating in the range proof. Depending on the Beta parameters chosen in the protocol implementation, the attack might require 16 signatures or more fully exfiltrate the other parties'

private key shares.

CVE-2023-33241 has been assigned by [H](#) disclosures@halborn.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [H](#) **GG TSS Implementations - Wallet** version = 18

Affected Vendor/Software: [H](#) **GG TSS Implementations - Wallet** version = 20

CVSS3 Score: **9.1 - CRITICAL**

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

CVE References

Description	Tags	Link
GG18 and GG20 Paillier Key Vulnerability [CVE-2023-33241]: Technical Report - Fireblocks	www.fireblocks.com text/html	MISC www.fireblocks.com/blog/gg18-and-gg20-paillier-key-vulnerability-technical-report/
GitHub - fireblocks-labs/mpc-ecdsa-attacks-23	github.com text/html	MISC github.com/fireblocks-labs/mpc-ecdsa-attacks-23
GitHub - fireblocks-labs/safeheron-gg20-exploit-poc	github.com text/html	MISC github.com/fireblocks-labs/safeheron-gg20-exploit-poc

[eprint.iacr.org
application/pdf](https://eprint.iacr.org/application/pdf)

 [MISC eprint.iacr.org/2020/540.pdf](https://eprint.iacr.org/2020/540.pdf)

[eprint.iacr.org
application/pdf](https://eprint.iacr.org/application/pdf)

 [MISC eprint.iacr.org/2019/114.pdf](https://eprint.iacr.org/2019/114.pdf)

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	Gg18 Project	Gg18	-	All	All	All
Application	Gg20 Project	Gg20	-	All	All	All
cpe:2.3:a:gg18_project:gg18:-:*****:						
cpe:2.3:a:gg20_project:gg20:-:*****:						

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 registered 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](#)