



CVE-2023-46324

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-46324
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-23 01:15:00 UTC
Updated	2023-10-30 13:46:00 UTC
Description	pkg/suci/suci.go in free5GC udm before 1.2.0, when Go before 1.19 is used, allows an Invalid Curve Attack because it may

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Free5gc	Udm	All	All	All	All
Application	Golang	Go	All	All	All	All

References

Reference	Source	Link	Tags
Prevent Invalid Curve Attack on 5G SUCI Feature by Roy-Hu · Pull Request #20 · free5gc/udm · GitHub	MISC	github.com	
Comparing v1.1.1...v1.2.0 · free5gc/udm · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995693](#) GO (Go) Security Update for github.com/free5gc/udm (GHSA-cqvv-r3g3-26rf)

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)