CVE-2023-20123

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-20123
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-05 19:15:00 UTC
Updated	2023-11-07 04:06:00 UTC
Description	A vulnerability in the offline access mode of Cisco Duo Two-Factor Authentication for macOS and Duo Authentication for W

Risk And Classification

Problem Types: CWE-294

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Duo	All	All	All	All
Application	Cisco	Duo Authentication For Windows Logon And Rdp	All	All	All	All

References

Reference	Source	Link
Cisco Duo Authentication for macOS and Duo Authentication for Windows Logon Offline Credentials Replay Vulnerability	CISCO	sec.c
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

379523 Cisco Duo Authentication for macOS and Duo Authentication for Windows Logon Offline Credentials Replay Vulnerability (cisco-sa-duo-replay-knuNKd)

Free CVE JSON API cve.report/api

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