



CVE-2023-29930

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

Summary

CVE	CVE-2023-29930
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-10 15:15:00 UTC
Updated	2023-05-24 13:50:00 UTC
Description	An issue was found in Genesys CIC Polycom phone provisioning TFTP Server all version allows a remote attacker to execute

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Genesys	Tftp Server	All	All	All	All

References

Reference	Source
GitHub - YSaxon/TFTPlunder: Exploit for CVE-2023-29930: blind file read/write in Genesys TFTP provisioning server configuration	MISC
Configuration of CIC Phone Features for Polycom Phones Technical Reference - Configure the TFTP Server	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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