CVE-2023-25000

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

Summary

CVE	CVE-2023-25000
State	PUBLIC
Assigner	security@hashicorp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-30 01:15:00 UTC
Updated	2023-05-26 20:15:00 UTC
Description	HashiCorp Vault's implementation of Shamir's secret sharing used precomputed table lookups, and was vulnerable to cach

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hashicorp	Vault	All	All	All	All
Application	Hashicorp	Vault	All	All	All	All

References

Reference	Source
HCSEC-2023-10 - Vault Vulnerable to Cache-Timing Attacks During Seal and Unseal Operations - Security - HashiCorp Discuss	MISC
March 2023 Hashicorp Vault Vulnerabilities in NetApp Products | NetApp Product Security	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.

Free CVE JSON API cve.report/api

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