CVE-2023-4680

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

Summary

CVE	CVE-2023-4680
State	PUBLIC
Assigner	security@hashicorp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-15 00:15:00 UTC
Updated	2023-09-20 14:55:00 UTC
Description	HashiCorp Vault and Vault Enterprise transit secrets engine allowed authorized users to specify arbitrary nonces, even with

Risk And Classification

Problem Types: CWE-20

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	S
HCSEC-2023-28 - Vault's Transit Secrets Engine Allowed Nonce Specified without Convergent Encryption - Security - HashiCorp Discuss	N
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995295 GO (Go) Security Update for github.com/hashicorp/vault (GHSA-v84f-6r39-cpfc)

Free CVE JSON API cve.report/api

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