



CVE-2021-27668

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

Summary

CVE	CVE-2021-27668
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-31 18:15:00 UTC
Updated	2022-09-08 21:48:00 UTC
Description	HashiCorp Vault Enterprise 0.9.2 through 1.6.2 allowed the read of license metadata from DR secondaries without authentication

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Score
HCSEC-2021-05 - Vault Enterprise's DR Secondaries Exposed License Metadata Without Authentication - Security - HashiCorp Discuss	Medium
HashiCorp Vault: Multiple Vulnerabilities (GLSA 202207-01) — Gentoo security	Good
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501705 Alpine Linux Security Update for vault
501933 Alpine Linux Security Update for vault
690215 Free Berkeley Software Distribution (FreeBSD) Security Update for vault (52bd2d59-4ab5-4bef-a599-7aac4e92238b)
710575 Gentoo Linux HashiCorp Vault Multiple Vulnerabilities (GLSA 202207-01)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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