



CVE-2020-25594

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-25594
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-01 16:15:00 UTC
Updated	2022-09-14 20:43:00 UTC
Description	HashiCorp Vault and Vault Enterprise allowed for enumeration of Secrets Engine mount paths via unauthenticated HTTP re

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
Application	Hashicorp	Vault	All	All	All	All
Application	Hashicorp	Vault	All	All	All	All

References

Reference
HCSEC-2021-03 - Vault API Endpoint Allowed Enumeration of Secrets Engine Mount Paths Without Authentication - Security - HashiCorp Dis
HashiCorp Vault: Multiple Vulnerabilities (GLSA 202207-01) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501704](#) Alpine Linux Security Update for vault

[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](#)