



CVE-2021-43998

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

Summary

CVE	CVE-2021-43998
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-30 15:15:00 UTC
Updated	2022-09-08 21:42:00 UTC
Description	HashiCorp Vault and Vault Enterprise 0.11.0 up to 1.7.5 and 1.8.4 templated ACL policies would always match the first-created alias per entity and auth backend.

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hashicorp	Vault	1.8.4	All	All	All
Application	Hashicorp	Vault	1.8.4	All	All	All
Application	Hashicorp	Vault	All	All	All	All
Application	Hashicorp	Vault	All	All	All	All

References

Reference

- [HCSEC-2021-30 - Vault's Templated ACL Policies Matched First-Created Alias Per Entity and Auth Backend - Security - HashiCorp Discuss](#)
- [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

[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](#)