



CVE-2022-36129

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

Summary

CVE	CVE-2022-36129
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-26 23:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	HashiCorp Vault Enterprise 1.7.0 through 1.9.7, 1.10.4, and 1.11.0 clusters using Integrated Storage expose an unauthenticated

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hashicorp	Vault	1.11.0	All	All	All
Application	Hashicorp	Vault	1.11.0	All	All	All
Application	Hashicorp	Vault	All	All	All	All
Application	Hashicorp	Vault	All	All	All	All

References

Reference
CVE-2022-36129 HashiCorp Vulnerability in NetApp Products NetApp Product Security
HCSEC-2022-15 - Vault Enterprise Does Not Verify Existing Voter Status When Joining An Integrated Storage HA Node - Security - HashiCorp
HashiCorp Discuss
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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