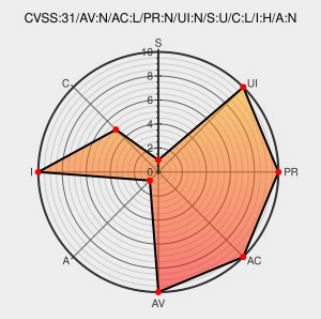
CVE-2020-16250

Published on: 08/26/2020 12:00:00 AM UTC

Last Modified on: 08/29/2023 05:13:00 PM UTC

CVE-2020-16250

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Vault from Hashicorp contain the following vulnerability:

HashiCorp Vault and Vault Enterprise versions 0.7.1 and newer, when configured with the AWS IAM auth method, may be vulnerable to authentication bypass. Fixed in 1.2.5, 1.3.8, 1.4.4, and 1.5.1..

CVE-2020-16250 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	HIGH	NONE

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
HashiCorp Blog: Vault	Product Vendor Advisory www.hashicorp.com text/html	MISC www.hashicorp.com/blog/category/vault/

vault/CHANGELOG.md at master · hashicorp/vault · GitHub	Release Notes Vendor Advisory github.com text/html	MISC github.com/hashicorp/vault/blob/master/CHANGELOG.md#151
Hashicorp Vault AWS IAM Integration Authentication Bypass ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159478/Hashicorp-Vault-AWS-IAM-Integration-Authentication-Bypass.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

501264 Alpine Linux Security Update for vault

501702 Alpine Linux Security Update for vault

981827 Go (go) Security Update for github.com/hashicorp/vault (GHSA-fp52-qw33-mfmw)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:hashicorp:vault:*:*:*:*:-:*:*:*:

cpe:2.3:a:hashicorp:vault:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:hashicorp:vault:*:*:*:*:-:*:*:*:

cpe:2.3:a:hashicorp:vault:*:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→