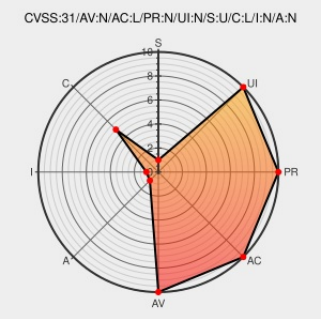
CVE-2020-7955

Published on: 01/31/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-7955

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



Certain versions of Consul from Hashicorp contain the following vulnerability:

HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.

CVE-2020-7955 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
HashiCorp Blog	Vendor Advisory www.hashicorp.com text/html	MISC www.hashicorp.com/blog/category/consul/
Add ACL enforcement to the v1/agent/health/service/* endpoints · Issue	Third Party Advisory	MISC

#7160 · hashicorp/consul · GitHub github.com text/html github.com/hashicorp/consul/issues/7160

Related QID Numbers

981946 Go (go) Security Update for github.com/hashicorp/consul (GHSA-r9w6-rhh9-7v53)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:hashicorp:consul:*:*:*:*:*:*:*:*:

cpe:2.3:a:hashicorp:consul:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:hashicorp:consul:*:*:*:*:*:*:*:*:

cpe:2.3:a:hashicorp:consul:*:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→