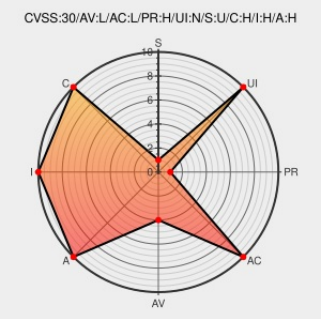
CVE-2020-3236

Published on: 06/17/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3236 - advisory for cisco-sa-nfvis-ptrav-SHMzzwVR

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



Certain versions of Enterprise Network Function Virtualization Infrastructure from Cisco contain the following vulnerability:

A vulnerability in the CLI of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files. The attacker would need valid administrative credentials. This vulnerability is due to improper input validation of CLI command arguments. An attacker could exploit this vulnerability by using path traversal techniques when executing a vulnerable command. A successful exploit could allow the attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files on an affected device.

CVE-2020-3236 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Enterprise NFV Infrastructure Software** version **n/a**

CVSS3 Score: 6.7 - MEDIUM

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Enterprise NFV Infrastructure Software Path Traversal Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200617 Cisco Enterprise NFV Infrastructure Software Path Traversal Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Enterprise Network Function Virtualization Infrastructure	All	All	All	All
Application	Cisco	Enterprise Network Function Virtualization Infrastructure	All	All	All	All

cpe:2.3:a:cisco:enterprise_network_function_virtualization_infrastructure:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:enterprise_network_function_virtualization_infrastructure:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→