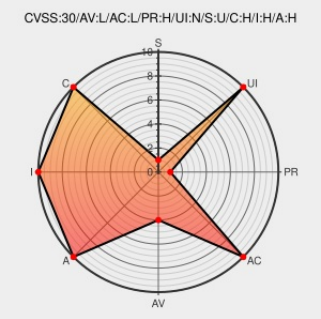
CVE-2019-1972

Published on: 08/08/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:47 PM UTC

CVE-2019-1972 - advisory for cisco-sa-20190807-nfv-privescal

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



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

A vulnerability the Cisco Enterprise NFV Infrastructure Software (NFVIS) restricted CLI could allow an authenticated, local attacker with valid administrator-level credentials to elevate privileges and execute arbitrary commands on the underlying operating system as root. The vulnerability is due to insufficient restrictions during the execution of an affected CLI command. An attacker could exploit this vulnerability by leveraging the insufficient restrictions during the execution of an affected command. A successful exploit could allow the attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root.

CVE-2019-1972 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 Privilege Escalation Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20190807 Cisco Enterprise NFV Infrastructure Software Privilege Escalation Vulnerability

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.

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→