



# CVE-2019-1971

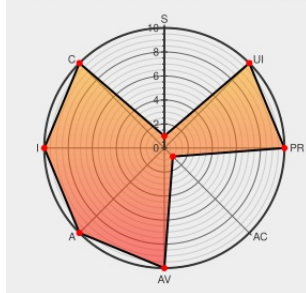
Published on: 08/08/2019 12:00:00 AM UTC

Last Modified on: 10/29/2021 06:37:00 PM UTC

## CVE-2019-1971 - advisory for cisco-sa-20190807-nfv-commandinj

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Enterprise Network Function Virtualization Infrastructure](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the web portal of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an unauthenticated, remote attacker to perform a command injection attack and execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the web portal framework. An attacker could exploit this

vulnerability by providing malicious input during web portal authentication. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.

CVE-2019-1971 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** 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: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **10 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
|                        |                   |                     |

COMPLETE

COMPLETE

COMPLETE

## CVE References

| Description                                                                  | Tags                                                                                            | Link                                                                                                        |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Cisco Enterprise NFV Infrastructure Software Command Injection Vulnerability | <a href="#">Vendor Advisory</a><br><a href="#">tools.cisco.com</a><br><a href="#">text/html</a> | <a href="#">CISCO 20190807 Cisco Enterprise NFV Infrastructure Software Command Injection Vulnerability</a> |

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](mailto: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

## Social Mentions

| Source | Title | Posted (UTC) |
|--------|-------|--------------|
|--------|-------|--------------|

[← Previous ID](#)[Next ID→](#)

© CVE.report 2023   |

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](#).

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