



Published on: 08/21/2019 12:00:00 AM UTC

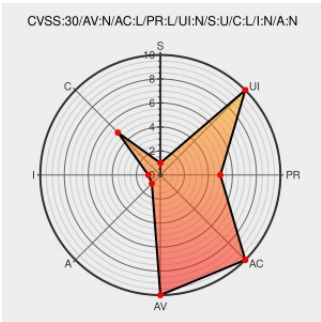
Last Modified on: 03/23/2021 11:27:42 PM UTC

CVE-2019-12623 - advisory for cisco-sa-20190821-nfv-enumeration

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

A vulnerability in the web server functionality of Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS) could allow an authenticated, remote attacker to perform file enumeration on an affected system. The vulnerability is due to the web server responding with different error codes for existing and non-existing files.

An attacker could exploit this vulnerability by sending GET requests for different file names. A successful exploit could allow the attacker to enumerate files residing on the system.

CVE-2019-12623 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 **3.12.1**

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco Enterprise Network Functions Virtualization Infrastructure Software File Enumeration Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20190821 Cisco Enterprise Network Functions Virtualization Infrastructure Software File Enumeration 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 Functions Virtualization Infrastructure	All	All	All	All
Application	Cisco	Enterprise Network Functions Virtualization Infrastructure	All	All	All	All
cpe:2.3:a:cisco:enterprise_network_functions_virtualization_infrastructure:*:*:*:*:*:						
cpe:2.3:a:cisco:enterprise_network_functions_virtualization_infrastructure:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← 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](#)