



# CVE-2021-34746

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-34746
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-09-02 03:15:00 UTC
<b>Updated</b>	2023-11-07 03:36:00 UTC
<b>Description</b>	A vulnerability in the TACACS+ authentication, authorization and accounting (AAA) feature of Cisco Enterprise NFV Infrastr

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Enterprise Nfv Infrastructure Software	All	All	All	All
Application	Cisco	Enterprise Nfv Infrastructure Software	4.5.1	All	All	All

## References

Reference	Source	Link
Cisco Enterprise NFV Infrastructure Software Authentication Bypass Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>
Cisco ENCS - Authentication Bypass (CVE-2021-34746) · Advisory · orangecertcc/security-research · GitHub	MISC	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[317027](#) Cisco Enterprise NFV Infrastructure Software Authentication Bypass Vulnerability

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](#)**