



CVE-2020-3446

Published on: 08/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

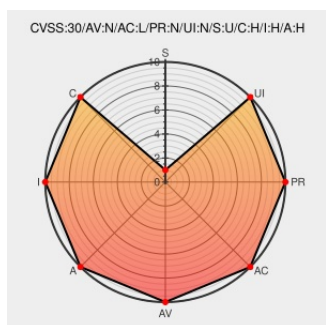
CVE-2020-3446 - advisory for cisco-sa-waas-encsw-cspw-cred-hZzL29A7

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Csp 5228-w](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in Cisco Virtual Wide Area Application Services (vWAAS) with Cisco Enterprise NFV Infrastructure Software (NFVIS)-bundled images for Cisco ENCS 5400-W Series and CSP 5000-W Series appliances could allow an unauthenticated, remote attacker to log into the NFVIS CLI of an affected device by using accounts that

have a default, static password. The vulnerability exists because the affected software has user accounts with default, static passwords. An attacker with access to the NFVIS CLI of an affected device could exploit this vulnerability by logging into the CLI. A successful exploit could allow the attacker to access the NFVIS CLI with administrator privileges.

CVE-2020-3446 has been assigned by [Cisco](#) 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 Wide Area Application Services (WAAS)** version n/a

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact	Impact	Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco vWAAS for Cisco ENCS 5400-W Series and CSP 5000-W Series Default Credentials Vulnerability	Vendor Advisory tools.cisco.com text/html	 CISCO 20200819 Cisco vWAAS for Cisco ENCS 5400-W Series and CSP 5000-W Series Default Credentials 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
Hardware 	Cisco	Csp 5228-w	-	All	All	All
Hardware 	Cisco	Csp 5228-w	-	All	All	All
Operating System	Cisco	Csp 5228-w Firmware	6.4\ (1\)	All	All	All
Operating System	Cisco	Csp 5228-w Firmware	6.4\ (3d\)	All	All	All
Operating System	Cisco	Csp 5228-w Firmware	6.4\ (1\)	All	All	All
Operating System	Cisco	Csp 5228-w Firmware	6.4\ (3d\)	All	All	All
Hardware 	Cisco	Csp 5436-w	-	All	All	All
Hardware 	Cisco	Csp 5436-w	-	All	All	All
Operating System	Cisco	Csp 5436-w Firmware	6.4\ (1\)	All	All	All
Operating System	Cisco	Csp 5436-w Firmware	6.4\ (3d\)	All	All	All
Operating System	Cisco	Csp 5436-w Firmware	6.4\ (1\)	All	All	All
Operating System	Cisco	Csp 5436-w Firmware	6.4\ (3d\)	All	All	All
Hardware 	Cisco	Encs 5406-w	-	All	All	All
Hardware 	Cisco	Encs 5406-w	-	All	All	All
Operating System	Cisco	Encs 5406-w Firmware	6.4\ (1\)	All	All	All
Operating	Cisco	Encs 5406-w Firmware	6.4\ (3d\)	All	All	All

Operating System	Cisco	Encs 5406-w Firmware	6.4\1\	All	All	All
Operating System	Cisco	Encs 5406-w Firmware	6.4\3d\	All	All	All
Hardware 🚩🔗	Cisco	Encs 5408-w	-	All	All	All
Hardware 🚩🔗	Cisco	Encs 5408-w	-	All	All	All
Operating System	Cisco	Encs 5408-w Firmware	6.4\1\	All	All	All
Operating System	Cisco	Encs 5408-w Firmware	6.4\3d\	All	All	All
Operating System	Cisco	Encs 5408-w Firmware	6.4\1\	All	All	All
Operating System	Cisco	Encs 5408-w Firmware	6.4\3d\	All	All	All
Hardware 🚩🔗	Cisco	Encs 5412-w	-	All	All	All
Hardware 🚩🔗	Cisco	Encs 5412-w	-	All	All	All
Operating System	Cisco	Encs 5412-w Firmware	6.4\1\	All	All	All
Operating System	Cisco	Encs 5412-w Firmware	6.4\3d\	All	All	All
Operating System	Cisco	Encs 5412-w Firmware	6.4\1\	All	All	All
Operating System	Cisco	Encs 5412-w Firmware	6.4\3d\	All	All	All
cpe:2.3:h:cisco:csp_5228-w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:csp_5228-w:-:*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5228-w_firmware:6.4\1\):*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5228-w_firmware:6.4\3d\):*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5228-w_firmware:6.4\1\):*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5228-w_firmware:6.4\3d\):*:*:*:*:*:						
cpe:2.3:h:cisco:csp_5436-w:-:*:*:*:*:*:						
cpe:2.3:h:cisco:csp_5436-w:-:*:*:*:*::~:						
cpe:2.3:o:cisco:csp_5436-w_firmware:6.4\1\):*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5436-w_firmware:6.4\3d\):*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5436-w_firmware:6.4\1\):*:*:*:*:*:						
cpe:2.3:o:cisco:csp_5436-w_firmware:6.4\3d\):*:*:*:*:*:						

cpe:2.3:h:cisco:encs_5406-w:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:encs_5406-w:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5406-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5406-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5406-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5406-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:encs_5408-w:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:encs_5408-w:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5408-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5408-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5408-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5408-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:encs_5412-w:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:cisco:encs_5412-w:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5412-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5412-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5412-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:cisco:encs_5412-w_firmware:6.4~::~~::~~::~~::~~::~~::~~:::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→