CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-041

Default Credentials Vulnerability in Cisco vWAAS

August 20, 2020 — v1.0

TLP:WHITE

History:

- *20/08/2020 — v1.0 – Initial publication*

Summary

On 19th of August, Cisco released a security advisory [1] for a vulnerability affecting Cisco ENCS 5400-W Series and CSP 5000-W Series appliances. They are affected, it they are running Cisco Virtual Wide Area Application Services (vWAAS) with Cisco Enterprise NFV Infrastructure Software (NFVIS)-bundled image releases 6.4.5, or 6.4.3d and earlier.

This vulnerability allows an unauthenticated, remote attacker to log into the NFVIS CLI of an affected device by using accounts that have a default, static password.

Cisco is not aware of any public announcements or malicious use of the vulnerability.

Technical Details

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.

Products Affected

These vulnerabilities affect several products:

- Cisco ENCS 5400-W Series releases 6.4.5, or 6.4.3d and earlier, with Cisco vWAAS and NFVIS bundled image;
- CSP 5000-W Series releases 6.4.5, or 6.4.3d and earlier, with Cisco vWAAS and NFVIS bundled image.

Products confirmed **not vulnerable**:

- Standalone NFVIS running on Cisco ENCS 5000 Series and Cisco CSP 5000 Series devices;

- Standalone vWAAS software or WAAS software running on Cisco Wide Area Virtualization Engine (WAVE) appliances.

Recommendations

Cisco has released software updates that address this vulnerability with 6.4.3e, 6.4.5a, and later releases [2].

In addition, Cisco noted that ENCS 5400-W Series and CSP 5000-W Series appliances do not support a direct upgrade to vWAAS 6.4.3e and 6.4.5a releases from earlier releases. In order to run a fixed release, there must be a fresh install with the required version of the Cisco WAAS Unified Package for ENCS 5400-W and CSP 5000-W appliances.

CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds

There are no known workarounds.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-encsw-cspw-cred-hZzL29A7

[2] https://software.cisco.com/download/home/280484571/type/280836712/release/6.4.3e