CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-018

Cisco Critical Vulnerability Affecting IOS XE Software

August 30, 2019 — v1.0

TLP:WHITE

History:

- *30/08/2019 — v1.0 – Initial publication*

Summary

A major vulnerability affecting CISCO IOS XE operating system has been disclosed. The vulnerability identified as CVE-2019-12643 allows a remote user to bypass authentication and gain full control of the device that is running an outdated version of REST API virtual service container. This CVE obtain the highest severity score of 10.

Technical Details

This vulnerability allows a remote user to obtain the `token-id` of an administrator already authenticated into the REST API by sending malicious HTTP requests to the vulnerable device. Then, the remote user can run some commands with high privileges [1].

To exploit this vulnerability, the administrator has to be authenticated and the device needs to run the outdated Cisco REST API virtual service container, which is not installed and enabled by default.

Products Affected

This vulnerability actually affected the following products :

- Cisco 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco Cloud Services Router 1000V Series
- Cisco Integrated Services Virtual Router

Recommendations

There are no workarounds to address this vulnerability. Cisco has released software updates to fix the defective software and for other issues [2]. Moreover, CISCO has released a new version of IOS XE that prevent from installing and enabling vulnerable version of REST API virtual service container.

References

[1] https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-bug-in-virtual-service-container-for-ios-xe/

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass