Security Advisory 2019-015

CSRF Vulnerability in Cisco IOS XE Software Web UI

June 14, 2019 — v1.0

TLP:WHITE

History:

- *14/06/2019 — v1.0: Initial publication*

Summary

A Cross-Site Request Forgery (CSRF) vulnerability in the web user interface (web UI) of CISCO IOS XE Software [1] was discovered. In some CISCO products, the web UI has insufficient CSRF protection. An attacker can potentially perform a CSRF operation against an authenticated user in the web UI. This could allow the attacker to perform actions on the device with the permissions of the victim.

Technical Details

CSRF is an attack that forces an end-user to execute unwanted actions on a web application in which they are currently authenticated [2]. An attacker can trick the victim to follow a malicious link and thus allow the attacker to perform actions on the device with the permissions of the victim. The vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software with the HTTP Server feature enabled. The risk depends on the version of the software.

Products Affected

System owners should use the CISCO IOS Software Checker [3] to determine if their devices are vulnerable.

Recommendations

- Disable HTTP Server until an update of the software is completed.
- Update the software following the vendor's guidelines [1].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190612-iosxe-csrf#fs

[2] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

[3] https://tools.cisco.com/security/center/softwarechecker.x