Advisory Alert

Alert Number: AAA20231031 **Date:** October 31, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Privilege Escalation Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical** – Initial release date **16th Oct 2023 (AAA20231017, AAA20231023)**
Affected Vulnerability	Privilege Escalation Vulnerabilities (CVE-2023-20198, CVE-2023-20273)
Description	Cisco has released a security remediation to address privilege escalation vulnerabilities in Cisco IOS XE Software. These vulnerabilities may initially allow an attacker to create a local user and password combination. After creating the local account the attacker may elevate privilege to root and write the implant to the file system. It is strongly recommends to apply the necessary remediation at your earliest to avoid issues.
Affected Products	Cisco IOS XE Software Release Train 17.9 Cisco IOS XE Software Release Train 17.6 Cisco IOS XE Software Release Train 16.12 (Catalyst 3650 and 3850 only)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.