KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature” (KSA-2023-3)

In October 2023, Cisco released a security advisory on two security vulnerabilities (“Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature”) affecting their Cisco IOS XE software. An attacker, who successfully exploits both vulnerabilities in sequence, can create a local account on an affected system and elevate their privilege to gain full control of the affected system.

For the affected products and services, Krones rates the likelihood of being exploited as medium to low. Therefore, timely action is recommended for devices exposed to untrusted networks such as the internet.

Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

No.	Likelihood of exploitation[1]	Affected products or services	Default state and remediation
1	Medium (default configuration) Very low (configuration modified by Krones)	Cisco FlexVPN routers, running Cisco IOS XE • Cisco C1111-4P • Cisco IR1101	• By default, the exploited feature is enabled on affected devices. However, remote access to FlexVPN routers is limited. • Krones modified the configuration of all commissioned FlexVPN routers that were reachable via VPN between 2023-10-16 and 2023-10-25, based on the official Cisco recommendation. • Krones will change the configuration of remaining FlexVPN routers during commissioning (managed by Krones).
2	Low	Cisco industrial switches, running Cisco IOS XE • Cisco IE 3300 • Cisco IE 4000 • Cisco 9200 • Cisco 9300 • Cisco C1000	• By default, the exploited feature is enabled on affected devices. However, these devices aren’t exposed to untrusted networks in their intended use case. • Krones may offer customer-specific solutions. Please get in touch with Krones LCS.
Krones may add additional affected products or services, or update remediations as soon as there is new information available.			

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Security contact

If you have any questions regarding this security advisory or other security-related questions, please contact the Product Security Incident Response Team (PSIRT) of Krones: cyber.security@krones.com

OpenPGP key for confidential messages:
https://www.krones.com/ext/securitytxt/cyber.security@krones.com.asc

Appendix A: Technical description of the security vulnerabilities

This section describes security vulnerabilities covered by this Krones Security Advisory. For each security vulnerability, Krones includes the following public information:

- **Description:** A brief description of the security vulnerability as mentioned in the original security advisory or in the National Vulnerability Database (NVD).
- **CVSS v3.1 Base Score:** The current CVSS v3.1 Base Score as mentioned in the original security advisory or in the National Vulnerability Database (NVD).
- **Listed in CISA Known Exploited Vulnerability Catalog:** Information whether the CISA KEV Catalog lists the security vulnerability. Being listed in the CISA KEV Catalog means that exploitation of the security vulnerability is publicly known. Krones recommends prioritizing handling security vulnerabilities listed in the CISA KEV Catalog.
- **EPSSv3 Score:** The current EPSSv3 Score as available via the FIRST EPSS API. Krones recommends prioritizing handling security vulnerabilities having a high EPSSv3 Score as this may indicate an increased likelihood of being exploited.

Vulnerability CVE-2023-20198

- **Description:** Cisco IOS XE Software Web UI Privilege Escalation Vulnerability, allowing an attacker to issue a privilege 15 command to create a local user and password combination.
- **CVSS v3.1 Base Score:** 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **Listed in CISA Known Exploited Vulnerability Catalog:** Yes
- **EPSSv3 Score:** Exploited

Vulnerability CVE-2023-20273

- **Description:** Unspecified vulnerability in Cisco IOS XE Software Web UI, allowing an attacker to elevate privilege to root and write their implant/malware to the file system.
- **CVSS v3.1 Base Score:** 7.2 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
- **Listed in CISA Known Exploited Vulnerability Catalog:** Yes
- **EPSSv3 Score:** Exploited

Appendix B: Further information

- Original security advisory by Cisco - Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature

Appendix C: Changelog

Version	Date	Changes
1.0	2023-10-18	Initial publication by the Krones PSIRT
1.1	2023-10-25	Updated summary of the vulnerabilities, updated technical description of CVE-2023-20198, added CVE-2023-20273