KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities, February 2025” (KSA-2025-1)

In February 2025, Cisco issued a security advisory regarding multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software. An authenticated, remote attacker could exploit these vulnerabilities to cause a denial of service (DoS) condition on affected devices.

For the affected products and services, Krones rates the likelihood of being exploited as low. Therefore, no specific action is required.

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	Very low	Cisco FlexVPN routers, running Cisco IOS XE • Cisco C1111-4P • Cisco IR1101	• By default, the exploited feature is enabled on affected devices. However, exploiting it would require credentials. • Krones will change the configuration of all FlexVPN routers for further hardening (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.
3	Low	Older, unsupported Cisco industrial switches • Cisco IE 3000 • Cisco 2960 • Cisco 3560 • Cisco 3650 • Cisco 3750 • Cisco 3850	• 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 recommends replacing the unsupported switches with the current generation. 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

Workarounds and mitigation

The following specific workarounds and mitigation are recommended in addition to the remediation measures listed above to further reduce the risk originating from the security vulnerabilities:

- Use firewalls to limit network traffic between networks, especially UDP ports 161 and 162.
- If applicable, monitor your complete network traffic to detect abnormal SNMP traffic.

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

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Appendix A: Technical description of the security vulnerabilities

This section outlines security vulnerabilities addressed by this Krones Security Advisory. For each vulnerability, or grouped identical vulnerabilities, Krones provides the following public information:

- **Description:** A brief description of the security vulnerability as mentioned in the original security advisory or in the MITRE CVE List.
- **CVSS v3.1 Base Score:** The current CVSS v3.1 Base Score as mentioned in the original security advisory or in the MITRE CVE List.
- **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.

Vulnerabilities CVE-2025-20169, CVE-2025-20170, CVE-2025-20171, CVE-2025-20173, CVE-2025-20174, CVE-2025-20175, CVE-2025-20176

- **Description:** A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.
- **CVSS v3.1 Base Score:** 7.7 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H)
- **Listed in CISA Known Exploited Vulnerability Catalog:** No
- **EPSSv3 Score:** 0.000440000

Vulnerability CVE-2025-20172

- **Description:** A vulnerability in the SNMP subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. For Cisco IOS and IOS XE Software, a successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. For Cisco IOS XR Software, a successful exploit could allow the attacker to cause the SNMP process to restart, resulting in an interrupted SNMP response from an affected device. Devices that are running Cisco IOS XR Software will not reload. This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.
- **CVSS v3.1 Base Scores:**
  - Cisco IOS, Cisco IOS XE: 7.7 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H)
  - Cisco IOS XR: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)
- **Listed in CISA Known Exploited Vulnerability Catalog:** No
- **EPSSv3 Score:** 0.000440000

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Appendix B: Further information

- Original security advisory by Cisco - Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities

Appendix C: Changelog

Version	Date	Changes
1.0	2025-02-10	Initial publication by the Krones PSIRT