KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Cisco IKEv2 Denial of Service Vulnerabilities, August 2025” (KSA-2025-2)

In August 2025, Cisco issued a security advisory regarding multiple vulnerabilities in their IKEv2 feature of Cisco IOS Software, Cisco IOS XE Software, Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, and Cisco Secure Firewall Threat Defense (FTD) Software. An unauthenticated, remote attacker could exploit these vulnerabilities to cause a denial of service (DoS) condition of 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	Low (unpatched) None (patched by Krones)	Cisco FlexVPN routers, running Cisco IOS XE • Cisco C1111-4P • Cisco IR1101	• By default, the exploited feature is enabled on affected devices. • Krones may offer customer-specific updates. Please get in touch with Krones LCS. • Krones continuously updates all actively-monitored Cisco routers that are online. • Krones updates remaining Cisco routers during commissioning (managed by Krones).
Krones advises regularly reviewing its Security Advisories for updates. Subscribe to Krones Security Advisories at Security Advisories - Krones.			

Security contact

For any inquiries related to this Krones Security Advisory, please contact the Krones Product Security Incident Response Team (PSIRT) at cyber.security@krones.com. To communicate confidentially, you may use our OpenPGP key, available here: krones.com/ext/securitytxt/cyber.security@krones.com.asc

[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

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:

- **Vulnerability description:** A description of the security vulnerability.
- **Rating on impact:** CVSS 3.1 Base Score or CVSS-B 4.0 score, if available.
- **Rating on exploitation:** This rating reflects known exploitation through publicly available sources, internal Krones Group knowledge, or inclusion in the CISA KEV Catalog. Alternatively, the EPSSv4 Score may be regarded as an indicator of exploitation likelihood.
- **Source:** Link to a public vulnerability source, if available.

Vulnerability CVE-2025-20253

- **Vulnerability description:** A vulnerability in the IKEv2 feature of Cisco IOS Software, IOS XE Software, Secure Firewall ASA Software, and Secure FTD Software could allow an unauthenticated, remote attacker to cause the device to reload, resulting in a DoS condition. This vulnerability is due to the improper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to cause an infinite loop that exhausts resources and could cause the device to reload.
- **Rating on impact:** CVSS 3.1 Base Score: 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
- **Rating on exploitation:** EPSSv4 Score: 0.001050000
- **Source:** https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ios-dos-DOESHWHy

Vulnerabilities CVE-2025-20239, CVE-2025-20225

- **Vulnerability description:** Two vulnerabilities in the IKEv2 feature of Cisco IOS Software, IOS XE Software, Secure Firewall ASA Software, and Secure FTD Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a DoS condition. These vulnerabilities are due to the improper processing of IKEv2 packets. An attacker could exploit these vulnerabilities by sending crafted IKEv2 packets to an affected device. A successful exploit of Cisco IOS and IOS XE Software could allow the attacker to cause a DoS condition, which would cause the affected device to reload. A successful exploit of Cisco Secure Firewall ASA and Secure FTD Software could allow the attacker to partially exhaust system memory, causing system instability such as being unable to establish new IKEv2 VPN sessions, which requires a manual reboot of the device to recover from this condition.
- **Rating on impact:** CVSS 3.1 Base Score: 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
- **Rating on exploitation:** EPSSv4 Score: 0.001050000
- **Source:** https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ios-dos-DOESHWHy

Changelog

Version	Date	Changes
1.0	2025-08-19	Originally released by the Krones Product Security Incident Response Team (PSIRT).