KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Avoiding misuse of the Cisco Smart Install feature” (KSA-2021-2)

To avoid misuse of the Smart Install (SMI) feature of various Cisco network devices, it is recommended to disable the feature. Cisco’s SMI provides zero-touch deployment for its network devices but can be misused if the feature remains enabled and the device is exposed to untrusted networks.

For the following devices, Krones rates the likelihood of being misused as low. Therefore, no specific action is required.

Affected devices

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

No.	Likelihood of misuse[1]	Affected devices	Default state and remediation
1	Low	Router Cisco 881	• By default, SMI is enabled. • The Cisco 881 is discontinued by Krones and Cisco. • Krones offers an upgrade to Cisco 1111. Please get in touch with Krones LCS.
2	Very low	Switches • Cisco 2960 • Cisco 3560 • Cisco 3650 • Cisco 3750 • Cisco IE2000 • Cisco IE3000 • Allen-Bradley Stratix 5700	• By default, SMI is enabled. • Krones offers customer-specific solutions. Please get in touch with Krones LCS.
3	None	Switches • Cisco 9200 • Cisco 9300 • Cisco IE3300	• SMI feature isn’t implemented. • No further action is required.
4	None	Router Cisco 1111	• SMI feature isn’t implemented. • No further action is required.
Krones may add additional devices, or update remediations as soon as there is new information available.			

[1] The likelihood of misuse 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 of misuse:

- Use firewalls to control traffic between IT/OT networks and production lines. Explicitly allow traffic (whitelisting). If applicable, block traffic on TCP port 4786.
- If applicable, monitor your complete network traffic to detect traffic to TCP port 4786 and outgoing TFTP traffic (UDP port 69) to the internet.

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: Further information

- Original security advisory by Cisco - Cisco Smart Install Protocol Misuse
- Detailed Cisco blog post about SMI - Cisco PSIRT – Mitigating and Detecting Potential Abuse of Cisco Smart Install Feature - Cisco Blogs

Appendix B: Changelog

Version	Date	Changes
1.0	2021-05-06	Initial publication by the Krones PSIRT
1.1	2021-05-19	Added the Cisco 3750 switch