KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Weak Key Protection Vulnerability in SIMATIC S7-1500” (KSA-2022-1)

In October 2022, Siemens published a security advisory regarding a weak key protection vulnerability in various SIMATIC S7 families. An attacker, who successfully exploits the vulnerability, can read the built-in global private key of the SIMATIC S7 family to then extract confidential configuration data from projects on the PLC or legacy communication of the PLC.

For the affected products and services, Krones rates the likelihood of being exploited as medium. Therefore, timely action is recommended.

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	Machines that use the SIMATIC S7-1500 PLC (only if software uses Krones release/Serienstand SE2019/09 or newer)	• We recommend implementing the mitigation listed below. • Krones may offer customer-specific solutions. Please get in touch with Krones LCS.
2	Medium	Steinecker/Krones process equipment that uses the SIMATIC S7-1500 PLC (brewery equipment)	• We recommend implementing the mitigation listed below. • Krones may offer customer-specific solutions. Please get in touch with Krones LCS.
3	Medium	System Logistics GmbH intralogistics equipment that uses the SIMATIC S7-1500 PLC	• We recommend implementing the mitigation listed below.
Krones may add additional affected products or services, or update remediations as soon as there is new information available.			

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 vulnerability:

- Use legacy (i.e., not TLS-based) PG/PC and HMI communication only in trusted network environments.
- Protect access to the TIA Portal project and CPU (including related memory cards) from unauthorized actors.
- Use firewalls to limit network traffic between Siemens PLCs and other networks (e.g., office network, internet). Only allow network traffic that is necessary for your production environment (e.g., MES, data analysis).
- If applicable, monitor your complete network traffic to detect abnormal traffic to Siemens PLCs.

[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 vulnerability

This section describes the vulnerability in detail. The CVSS v3.1 base score is the current severity rating according to the original security advisory by Siemens and does not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2022-38465

Affected Siemens S7-1500 protect the built-in private key insufficiently, allowing attackers to discover the private key of the S7-1500 product family. Attackers can conduct further attacks based on this knowledge, such as extracting confidential configuration data from projects or attacking the legacy PG/PC and HMI communication.

The CVSS v3.1 score for the vulnerability is 9.3
(CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C).

Appendix B: Further information

- Original security advisory by Siemens - SSA-568427_V1.0 (siemens.com)
- Additional remarks by Siemens - SSB-898115 (siemens.com)

Appendix C: Changelog

Version	Date	Changes
1.0	2022-11-11	Initial publication by the Krones PSIRT