KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Memory Protection Bypass Vulnerability in SIMATIC S7-1500” (KSA-2021-3)

In May 2021, Siemens published a security advisory regarding a memory protection bypass vulnerability in various SIMATIC S7 families. An attacker, who successfully exploits the vulnerabilities, can potentially write arbitrary data and code to protected memory areas or read sensitive data of affected PLCs.

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 mitigations listed below. • Customers may install the latest SIMATIC S7-1500 firmware 2.9.2 on their own. • Krones offers updating the affected S7-1500 devices. 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 mitigations listed below. • Customers may install the latest SIMATIC S7-1500 firmware 2.9.2 on their own. • Krones offers updating the affected S7-1500 devices. 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 mitigations listed below. • System Logistics GmbH may offer customer-specific solutions. Please get in touch with System Logistics Customer Service.
	Krones may add additional affected products or services, or update remediations as soon as there is new information available.		

Workarounds and mitigations

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

[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

- Use firewalls to limit network traffic between Siemens PLCs (TCP port 102) 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 TCP port 102.

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 vulnerabilities

This section describes each 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-2020-15782

A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks. The vulnerability affects all SIMATIC S7-1500 firmware versions prior to 2.9.2.

The CVSS v3.1 score for the vulnerability is 8.1
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C).

Appendix B: Further information

- Original security advisory by Siemens - https://cert-portal.siemens.com/productcert/pdf/ssa-434534.pdf

Appendix C: Changelog

Version	Date	Changes
1.0	2021-06-22	Initial publication by the Krones PSIRT
1.1	2021-07-07	Firmware updates can be applied for Steinecker/Krones process equipment
1.2	2021-07-20	Added remediation for equipment by System Logistics GmbH