KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “WannaCry/NotPetya” (KSA-2017-1)

In 2017, two global ransomware attacks have been observed. In May 2017, ransomware known as “WannaCry” infected more than 230,000 computers across 150 countries. One month later, “NotPetya” infected mostly systems in Ukraine, but also in other countries. In both cases, the malware tried to spread to other systems by exploiting a security vulnerability in the SMB (Server Message Block) protocol. Then, the malware started to encrypt files of the infected systems, and finally demanded ransom to allow the victim to decrypt the files.

For the affected products and services, Krones rates the likelihood of being exploited as high. Therefore, urgent 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	High	HMI systems based on Windows XP Embedded with image version: • IDC 1.xx / IDC 3.xx • IRX 1.xx / IRX 2.xx • MAX 1.xx / MAX 2.xx / MAX 3.xx • OSS 5.xx • OSR 4.xx	• Deploy image provided by Krones (Windows XP SP3 only) • Older systems (Windows XP SP2 or below as used by image versions OSX/IPX) require a hardware upgrade first. Krones offers Retrofit packages via LCS. • Krones offers whitelisting solutions via LCS
2	High	HMI systems based on Windows Embedded Standard 7 with image version: • IDC 4.xx • INS 1.xx • IRS 1.xx • SAM 1.xx	• Deploy image provided by Krones (Windows 7 only) • Krones offers whitelisting solutions via LCS
3	High	SitePilot • MES 7.*/8.* • former SitePilot versions (LMS, LDS, KAM)	Install patches provided by Microsoft as there are no known issues regarding compatibility (please be aware that required system restarts might lead to gaps in data acquisition). However, as operation of IT systems is not within the scope of responsibility of Krones/Syskron, we cannot guarantee that the system will operate flawlessly after updating Windows.

[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

4	High	IRIS (using iPanel touch display, and APC620/APC810) based on Windows XP Embedded: • ENYA • FIONA • GLORIA	• Patches can be deployed by Krones service technicians • Krones offers whitelisting solutions via LCS
5	High	DART based on Windows XP Embedded and software version: • 4.x • 5.x	• Update to DART 4.02.03c or 5.00.00SP7 • Krones offers whitelisting solutions via LCS
6	High	PCS systems (BOTEC)	• Use whitelisting (deployed on systems delivered from 2012 onwards) • Keep the system isolated • Krones offers a security check for these systems via LCS
7	High	Krones Pasteurizer (using SIMATIC IPC627C) based on Windows XP Embedded and image version: • PGA 1.xx.x (PGA 1.02.00) • PGC 1.xx.x (PGC 1.04.00)	• Deploy image provided by Krones (Windows XP SP3 only) • Older systems (Windows XP SP2 or below) require a hardware upgrade first
8	High	Krones Pasteurizer (using SIMATIC IPC) based on Windows Embedded Standard 7 and image version: • PGA 4.xx.x (PGA 4.01.00) • PGD 1.xx.x	Deploy image provided by Krones (Windows 7 only)

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:

- Krones recommends installing patches mentioned in Microsoft Security Bulletin MS17-010 immediately.
- If you use unsupported Microsoft platforms, please promptly review, download, test, and apply patches available in the Microsoft Update Catalog (KB4012598).

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 vulnerabilities

Vulnerability #1 (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148 are vulnerabilities in Microsoft's implementation of the Server Message Block 1 (SMBv1) protocol that allow remote attackers to execute arbitrary code via crafted packets. WannaCry and NotPetya ransomware utilize an exploit called EternalBlue that was leaked in April 2017. It exploits CVE-2017-0144 to execute arbitrary code on the target computer. Microsoft started to offer patches for all then-supported Windows systems in March 2017. Later, Microsoft also supplied patches for unsupported operating systems like Windows XP.

The CVSS v3.0 base score for the vulnerabilities is 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). For systems that can be patched, the temporal score results in 7.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C).

Vulnerability #2 (CVE-2017-0147)

CVE-2017-0147 is a vulnerability in Microsoft's implementation of the Server Message Block 1 (SMBv1) protocol that allows remote attackers to remotely disclose information from a server via crafted packets. Microsoft started to offer a patch for all then-supported Windows systems in March 2017.

The CVSS v3.0 base score for the vulnerability is 5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). For systems that can be patched, the temporal score results in 5.2 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C).

Appendix B: Further information

- Microsoft Security Bulletin MS17-010 - https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Appendix C: Changelog

Version	Date	Changes
2.0	2019-03-21	Initial publication by Krones PSIRT, based on previous WannaCry advisory 1.6 (2018-11-15) and Petya/NotPetya advisory 1.0 (2017-06-28) using an updated advisory template