KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Remote Desktop Services vulnerability in old versions of Windows (BlueKeep)” (KSA-2019-2)

On May 14, 2019, the Microsoft Security Response Center (MSRC) published an article regarding a vulnerability in Remote Desktop Services of old versions of Windows, also known as “BlueKeep”. At the same time, Microsoft released security updates for Windows XP SP3, Windows 7, Windows Server 2003 SP2, Windows Server 2008, and Windows Server 2008 R2. Newer versions of Windows like 8, 10, and Server 2012 (or newer) aren’t vulnerable. An attacker, who successfully exploits this vulnerability, can control the vulnerable Windows system completely, according to the MSRC. This includes installing/disabling/removing arbitrary software, and other malicious activities.

For some of 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	SitePilot • MES 7.*/8.*/9.*/10.* • 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.
2	Medium	PCS systems (BOTEC)	• Keep the system isolated. • Krones offers a security check for these systems via LCS (including security updates for the operating system).
3	Low	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	• Remote Desktop Services (RDS) are disabled by default. • Keep RDS disabled.

[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	Low	HMI systems based on Windows Embedded Standard 7 with image version: • IDC 4.xx • INS 1.xx • IRS 1.xx • SAM 1.xx	• Remote Desktop Services (RDS) are disabled by default. • Keep RDS disabled.
5	Low	Krones Pasteurizer (using SIMATIC IPC627C) based on Windows XP Embedded and image version: • PGA 1.x • PGC 1.x	• Remote Desktop Services (RDS) are disabled by default. • Keep RDS disabled.
6	Low	Krones Pasteurizer (using SIMATIC IPC) based on Windows Embedded Standard 7 and image version: • PGA 4.x • PGD 1.x	• Remote Desktop Services (RDS) are disabled by default. • Keep RDS disabled.
7	Low	DART based on Windows XP Embedded and software version: • 4.x • 5.x	• Remote Desktop Services (RDS) are disabled by default. • Keep RDS disabled.
Krones may add additional affected products/services, and 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:

- Krones recommends installing patches mentioned by MSRC in “Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)” immediately.
- If applicable, enable Network Level Authentication (NLA) on Windows 7, Windows Server 2008, and Windows Server 2008 R2.
- If applicable, block network traffic over TCP port 3389.
- If applicable, disable Remote Desktop Services (or Terminal Services resp.) completely.

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

This section describes each vulnerability in detail. The CVSS v3.0 base score is the current severity rating according to the National Vulnerability Database (NIST) and does not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2019-0708 (“BlueKeep”)

CVE-2019-0708 (also known as “BlueKeep”) is a vulnerability in the Remote Desktop Services (formerly known as Terminal Services) that affects older versions of Windows, including Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2. An unauthenticated attacker can send specially crafted packets to a vulnerable host to execute arbitrary code on the host without any user interaction.

Newer Windows versions, including Windows 8, Windows 10, and Windows Server 2012 (or newer) aren’t affected by CVE-2019-0708. The Remote Desktop Protocol (RDP) itself isn’t vulnerable.

The CVSS v3.0 base score for the vulnerability is 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). The current CVSSv3 temporal score is:

- Windows XP: 9.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C)
- Other affected Windows systems: 8.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C)

Krones rated the environmental scores for HMI/DART systems separately since RDS is disabled by default and must be actively enabled before the vulnerability can be exploited. The resulting CVSSv3 scores are:

- Windows XP: 5.9 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:X/MAC:H/MPR:H/MUI:R/MS:X/MC:X/MI:X/MA:X)
- Windows 7: 5.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:X/MAC:H/MPR:H/MUI:R/MS:X/MC:X/MI:X/MA:X)

Appendix B: Further information

- Prevent a worm by updating Remote Desktop Services (CVE-2019-0708) - https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
- CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Appendix C: Changelog

Version	Date	Changes
1.0	2019-05-22	Initial publication by the Krones PSIRT
1.1	2019-05-23	Added information regarding several HMI and DART systems
1.2	2019-07-26	Added Windows 2000 and Windows Server 2003 R2 to vulnerable systems. Updated remediations for PCS systems (BOTEC).