KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “BlueKeep-like vulnerabilities in Remote Desktop Services of current Windows versions (DejaBlue)” (KSA-2019-3)

On August 13, 2019, the Microsoft Security Response Center (MSRC) published an article regarding two vulnerabilities in Remote Desktop Services of current versions of Windows. According to the article, these vulnerabilities are like “BlueKeep” (see KSA-2019-2) but affect current versions of Windows. Microsoft published two additional security advisories regarding similar vulnerabilities in their newest Windows versions. The media names the vulnerabilities “DejaBlue”.

In total, there are two BlueKeep-like vulnerabilities in Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016, while all supported versions of Windows 10, including server versions (Windows Server 2019), contain four BlueKeep-like vulnerabilities in Remote Desktop Services.

Windows XP, Windows Server 2003, and Windows Server 2008 are not affected, nor is the Remote Desktop Protocol (RDP) itself affected.

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).

[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	HMI systems based on Windows 10 LTSB 2016 Build 1607.	• 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.
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 “Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019-1181/1182)” as well as patches for CVE-2019-1222/CVE-2019-1226 immediately.
- If applicable, enable Network Level Authentication (NLA) on all Windows-based systems.
- If applicable, block network traffic over TCP port 3389.
- If applicable, disable Remote Desktop Services 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

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.

Vulnerabilities CVE-2019-1181, and CVE-2019-1182

CVE-2019-1181, and CVE-2019-1182 are vulnerabilities in the Remote Desktop Services that affect all current versions of Windows, including Windows 7 SP1, Windows 8.1, Windows RT 8.1, Windows 10, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and all Windows-10-based Windows Server editions. An unauthenticated attacker can send specially crafted packets to a vulnerable host to execute arbitrary code on the host without any user interaction.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Windows 7 SP1 and Windows Server 2008 R2 SP1 are only affected if either RDP 8.0 or RDP 8.1 is installed.

Older Windows versions, including Windows XP, Windows Server 2003, and Windows Server 2008 aren't affected by the vulnerabilities. The Remote Desktop Protocol (RDP) itself isn't vulnerable.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). The current CVSSv3.0 temporal score is 8.8 (CVSS:3.0/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 systems separately since RDS is disabled by default and must be actively enabled before the vulnerability can be exploited (admin privileges required). The resulting CVSS 3.1 score for these systems is 6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/MPR:H/MUI:R).

Vulnerabilities CVE-2019-1222, and CVE-2019-1226

CVE-2019-1222, and CVE-2019-1226 are vulnerabilities in the Remote Desktop Services that affect the latest versions of Windows, including Windows 10, Windows Server 2019, and all Windows-10-based Windows Server editions. An unauthenticated attacker can send specially crafted packets to a vulnerable host to execute arbitrary code on the host without any user interaction.

Older Windows versions aren't affected by the vulnerabilities. The Remote Desktop Protocol (RDP) itself isn't vulnerable.

The CVSS v3.0 base score for the vulnerability is 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). The current CVSSv3.0 temporal score is 8.8 (CVSS:3.0/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 systems separately since RDS is disabled by default and must be actively enabled before the vulnerability can be exploited (admin privileges required). The resulting CVSS 3.1 score for these systems is 6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/MPR:H/MUI:R).

Appendix B: Further information

- Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019-1181/1182) - https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
- CVE-2019-1181 | Remote Desktop Services Remote Code Execution Vulnerability - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
- CVE-2019-1182 | Remote Desktop Services Remote Code Execution Vulnerability - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
- CVE-2019-1222 | Remote Desktop Services Remote Code Execution Vulnerability - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
- CVE-2019-1226 | Remote Desktop Services Remote Code Execution Vulnerability - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226

Appendix C: Changelog

Version	Date	Changes
1.0	2019-08-14	Initial publication by the Krones PSIRT