# Advisory 2019-03: Remote Code Execution in Remote Desktop Service

| | |
|---|---|
| Publication Date | 17/05/2019 |
| Last Update | 03/09/2019 |
| Current Version | 1.4 |
| Relevance | High |
| Related CVE | CVE-2019-0708 |

## Summary

A KnowledgeBase article [1] of Microsoft describes a remote code execution vulnerability within the Remote Desktop Service.

## Appearance

Beckhoff IPCs with Microsoft Operating Systems like Windows XP, Windows Server 2003 SP2, Windows XP Embedded SP3 and Windows Embedded Standard 2009 as well as Windows 7, Windows 2008 R2, and Windows 2008.

## Description

On Mai 14th, 2019 Microsoft published a blog article [1] about remote execution via Remote Desktop Service. This can be misused to run malware on devices that are reachable over the network and have Remote Desktop Service enabled.
Operating system updates are available for

- Windows 2003 and Windows XP [2]
- Windows 7, Windows 2008 R2, and Windows 2008 [3]

## Solution

Beckhoff has evaluated the patches from Microsoft for use with Beckhoff TwinCAT (TwinCAT 3.1 Build 4022.30 and TwinCAT 2 Build 2304) and found no real-time performance impacts.
Beckhoff takes this as an indication that applying these patches does not harm the real-time capabilities. However, Beckhoff cannot foresee all changes of the patch on all variations of software in the field.

Please note that this patch contains KB4499175 from Microsoft. For older TwinCAT versions, this means that the handling of Advisory 2019-01 [4] must be applied.

### Install Microsoft operating system updates

Beckhoff recommends creating a backup before installing updates so that the previous status can be restored at any time. This can be achieved with the Beckhoff Service Tool:
https://www.beckhoff.com/english.asp?industrial_pc/bst.htm
This operating system update for Windows can be retrieved from [2] and [3].

Disclaimer: Beckhoff is not responsible for any side effects negatively affecting the real-time capabilities of your TwinCAT control application possibly caused by updates. Beckhoff offers update images with qualified

**Beckhoff Automation** GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-securityincident@beckhoff.com
www.beckhoff.com

performance for Beckhoff hardware from time to time. TwinCAT System Manager offers tools, which can be of assistance to verify real-time performance after update. Only administrators or IT experts should perform the backup and update procedure

**Mitigation**

If the solution is not applicable due to own tests, Beckhoff recommends to

- Disable Remote Desktop Services if not required.
- Block Port 3389 in perimeter firewall

## Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

## Additional Resources

[1] Microsoft Publication: https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

[2] Microsoft Patches for Windows 2003 and Windows XP
https://support.microsoft.com/de-de/help/4500705/customer-guidance-for-cve-2019-0708

[3] Microsoft Patches for Windows 7, Windows 2008 R2, and Windows 2008
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[4] Spectre-V2 and impact on application performance as well as TwinCAT compatibility
https://download.beckhoff.com/download/Document/product-security/Advisories/advisory-2019-001.pdf

## History

| | | |
|---|---|---|
| V 1.0 | 17/05/2019 | Publication |
| V 1.1 | 22/05/2019 | Enhanced information regarding affected systems |
| V 1.2 | 29/05/2019 | Test Results for TwinCAT compatibility added |
| V 1.3 | 15/07/2019 | Added detailed TwinCAT versions of tests |
| V 1.4 | 03/09/2019 | Updated references |