SSB-501863: Customer Information on Microsoft Windows RDP Vulnerability for Siemens Healthineers

Publication Date: 2019-05-16
Last Update: 2019-05-22
Current Version: V1.1

SUMMARY

Microsoft released updates for several versions of Microsoft Windows, which fix a vulnerability in the Remote Desktop Service. The vulnerability could allow an unauthenticated remote attacker to execute arbitrary code on the target system if the system exposes the service to the network.

Several Siemens Healthineers products are based on Microsoft Windows, or can be installed on Microsoft Windows.

Some of these Siemens Healthineers products are affected by this vulnerability. Depending on the target system and intent of the attacker, a successful exploit could result in data corruption and potential harm for patients and/or the environment.

This document provides general information and recommendations for customers regarding the vulnerability.

DESCRIPTION

Microsoft released updates for Windows XP, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2 on 2019-05-14. The updates fix a vulnerability that affects the Remote Desktop Protocol (RDP) implementation on these operating systems.

The vulnerability could allow an unauthenticated remote attacker to execute arbitrary code on the target system. Depending on the target system and intent of the attacker, this could result in data corruption and potential harm for patients and/or the environment.

The Remote Desktop Service must be activated, and an attacker must have network access to port 3389/tcp of affected devices and NLA must de-activated at the same time in order to exploit the vulnerability.

The vulnerability is identified as CVE-2019-0708.

Microsoft has released updates that address the vulnerability and has released additional guidance for operators:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

At the time of publication of this bulletin, no exploitation of this security vulnerability has been publicly reported. However there is evidence that the security research community is working on an exploit and that such an exploit would eventually have adverse effects.

GENERAL RECOMMENDATIONS

For your general IT environment, please follow the recommendations of Microsoft regarding this vulnerability.

For Siemens Healthineers products, product specific advisories will be published when necessary.

For products that are End of Support, no updates are planned. Hence Siemens strongly recommends closing the RDP port where possible or disconnecting these devices from the network.

ADDITIONAL RESOURCES

A description of CVE-2019-0708 by Microsoft can be found here:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

The customer guidance for CVE-2019-0708 by Microsoft (including XP and Server 2003) can be found here:

https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2019-05-16):	Publication Date
V1.1 (2019-05-22):	Clarified End of Support products and possible impact

TERMS OF USE

Siemens Security Bulletins are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.