SSA-406175: Vulnerability in Siemens Healthineers Software Products

Publication Date:	2019-05-24
Last Update:	2019-05-24
Current Version:	V1.0
CVSS v3.0 Base Score:	9.8

SUMMARY

Microsoft has released updates for Windows XP, Windows 7, Windows Server 2008, and Windows Server 2008 R2 to fix a vulnerability in the Remote Desktop Service. The vulnerability could allow an unauthenticated remote attacker to execute arbitrary code in the target system if the system exposes the service to the network.

Some Siemens Healthineers software products are affected by this vulnerability. The exploitability of the vulnerability depends on the specific configuration and deployment environment of each product.

Siemens Healthineers recommends installing the appropriate security patches released by Microsoft. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
MagicLinkA: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
MagicView1000W: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

MagicView300: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
Medicalis Clinical Decision Support: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
Medicalis Intelligo: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
Medicalis Referral Management: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
Medicalis Workflow Orchestrator: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

Screening Navigator: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo Dynamics: VA10 and earlier	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo Imaging: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo Plaza: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo Workflow MLR: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

syngo Workflow SLR: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo.via: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo.via View&GO: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
syngo.via WebViewer: All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
teamplay (receiver software only): All versions	Apply all the appropriate security patches released by Microsoft. • Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. • The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

WORKAROUNDS AND MITIGATIONS

Siemens Healthineers has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Frequently update antivirus patterns.
- Ensure secure deployment of the device according to the intended use and configuration.

GENERAL SECURITY RECOMMENDATIONS

In addition, Siemens Healthineers recommends the following:

- Ensure you have appropriate backups and system restoration procedures.
- For specific patch and remediation guidance information, contact your local Siemens Healthineers customer service engineer, portal or our Regional Support Center.

PRODUCT DESCRIPTION

Healthcare digitalization software products from Siemens Healthineers are used in clinical environments.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2019-0708

An unauthenticated attacker with access to port 3389/tcp in an affected device may execute arbitrary commands with elevated privileges.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected device. No user interaction is required to exploit this vulnerability. The vulnerability impacts the confidentiality, integrity, and availability of the affected device.

CVSS v3.0 Base Score	9.8
CVSS Vector	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

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 (2019-05-24):	Publication Date

TERMS OF USE

Siemens Security Advisories 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.