SSA-166360: Vulnerability in Advanced Therapy Products from Siemens Healthineers

Publication Date: 2019-05-24
Last Update: 2019-07-09
Current Version: V1.1
CVSS v3.0 Base Score: 9.8

SUMMARY

Microsoft has 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.

Some Advanced Therapy products from Siemens Healthineers are affected by this vulnerability. The exploitability of the vulnerability depends on the actual configuration and deployment environment of each product.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SYSTEM ACOM.NET, Mat. Nr. 04815549: VC20A, VC21B, VC22B and VX22A	Disable Remote Desktop Protocol (RDP)
System ACOM.net 2.0, Mat. Nr. 05568386: VC20A, VC21B, VC22B and VX22A	Disable Remote Desktop Protocol (RDP)
System ACOM-Net, Mat. Nr. 5903872: VC20A, VC21B, VC22B and VX22A	Disable Remote Desktop Protocol (RDP)
Sensis SIS Server Machine, Mat. Nr. 06648153: VC11D, VC12M, VD11B	Update to AX037/19/P
Sensis SIS Server Machine, Mat. Nr. 06648153: VC11C	Upgrade to VC11D before applying update AX037/19/P
Sensis SIS Server Machine, Mat. Nr. 06648153: VC12B/C and VC12L	Upgrade to VC12M before applying update AX037/19/P
Sensis SIS Server Machine, Mat. Nr. 06648153: VD11A	Upgrade to VD11B before applying update AX037/19/P
Sensis High End SIS Server, Mat. Nr. 10140973: VC11D, VC12M	Update to AX037/19/P
Sensis High End SIS Server, Mat. Nr. 10140973: VC11C	Upgrade to VC11D before applying update AX037/19/P
Sensis High End SIS Server, Mat. Nr. 10140973: VC1B/C, VC12L	Upgrade to VC12M before applying update AX037/19/P

SENSIS Dell High-End Server (VC12), Mat. Nr. 10910620: VC12M	Update to AX037/19/P
SENSIS Dell High-End Server (VC12), Mat. Nr. 10910620: VC12B/C, VC12L	Upgrade to VC12M before applying the update AX037/19/P
VM SIS Virtual Server, Mat. Nr. 10765502: VC12M	Update to AX037/19/P
VM SIS Virtual Server, Mat. Nr. 10765502: VC12L	Upgrade to VC12M before applying the update AX037/19/P

WORKAROUNDS AND MITIGATIONS

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

- Contact Siemens Service Technician to disable Remote Desktop Protocol (RDP) on the product
- If possible, block port 3389/tcp on an external firewall.
- Secure the surrounding environment according to the recommendations provided by Microsoft which can be found here: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708.

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

Siemens Healthineers Advanced Therapies (AT) products are used in interventional laboratories and (hybrid) ORs for diagnostic and therapeutic procedures.

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
V1.1 (2019-07-09):	Added mitigation and clarified affected versions.

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.