SSA-832947: Vulnerability in Laboratory Diagnostics 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.

The majority of Laboratory Diagnostic products are not affected by this vulnerability. However, some products are affected and listed below. The exploitability of the vulnerability depends on the actual configuration and deployment environment of each product.

At the time of advisory publication no public exploitation of this security vulnerability was known.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Atellica Solution: All versions	Network Level Authentication (NLA) is enabled by default and is a mitigation for this vulnerability. The Microsoft patch will be in version 1.20 available in Q3 of calendar year 2019.
Aptio by Siemens: All versions	Patch will be available after September.
Aptio by Inpeco: All versions	Patch will be available after July.
StreamLab: All versions	Please contact customer service for mitigation information after July.
CentraLink: All versions	Customer bulletin 10810542 Revision 91 was released on May 24, 2019. The Microsoft patch can be applied by customers. The customer bulletin can be retrieved from the Laboratory Diagnostics and Point of Care Document Library https://www.siemens.com/document-library
syngo Lab Process Manager: All versions	Please contact customer service for mitigation information after July.
Viva E: All versions	Patch will be available after August.
Viva Twin: All versions	Patch will be available after August.

Atellica COAG 360: All versions on Windows 7	Apply patch or alternatively contact customer service for patch installation. https://doclib.healthcare.siemens.com/home
Atellica NEPH 630: All versions on Windows 7	Apply patch or alternatively contact customer service for patch installation. https://doclib.healthcare.siemens.com/home
BCS XP: All versions on Windows 7	Apply patch or alternatively contact customer service for patch installation. https://doclib.healthcare.siemens.com/home
BCS XP: All versions on Windows XP	Patch is available, contact customer service for installation.
BN ProSpec: All versions on Windows 7	Apply patch or alternatively contact customer service for patch installation. https://doclib.healthcare.siemens.com/home
BN ProSpec: All versions on Windows XP	Patch is available, contact customer service for installation.
CS 2000 (supported by Sysmex - for information only): All versions on Windows 7	Patch is available, contact customer service for installation.
CS 2000 (supported by Sysmex - for information only): All versions on Windows XP	Please contact customer service for countermeasures or available workaround information.
CS 2100 (supported by Sysmex - for information only): All versions on Windows 7	Patch is available, contact customer service for installation.
CS 2100 (supported by Sysmex - for information only): All versions on Windows XP	Please contact customer service for countermeasures or available workaround information.
CS 2500 (supported by Sysmex - for information only): All versions on Windows 7	Patch is available, contact customer service for installation.
CS 5100 (supported by Sysmex - for information only): All versions on Windows 7	Patch is available, contact customer service for installation.

WORKAROUNDS AND MITIGATIONS

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

- If possible, block port 3389/TCP on an external firewall.
- Secure the surrounding environment according to the recommendations provided by Microsoft to minimize the risk.
- For Siemens products that install on customer computers, customers are encouraged to secure those computers as soon as possible with the appropriate patches from Microsoft.

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 Laboratory Diagnostics products are used in diagnostics laboratories for immunoassay, chemistry, hematology, hemostasis, and plasma protein testing, in conjunction with automation and informatics.

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):	Removed CS 5100 for Windows XP, added patch information

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.