SSA-187667: DejaBlue Vulnerabilities - Siemens Healthineers Products

Publication Date: 2019-09-10
Last Update: 2019-09-10
Current Version: V1.0
CVSS v3.0 Base Score: 9.8

SUMMARY

Microsoft has released updates for several versions of Microsoft Windows, which fix vulnerabilities in the Remote Desktop Service that are discussed under the name DejaBlue. The vulnerabilities could allow an unauthenticated remote attacker to execute arbitrary code on the target system if the system exposes the service to the network.

All Siemens Healthineers products from all business lines have been evaluated. Most Siemens Healthineers products are not affected by the vulnerabilities because they do not provide the option to activate the Remote Desktop Service, implement other controls that mitigate the vulnerabilities, use a version of Microsoft Windows that is not affected, or are not based on Microsoft Windows.

This advisory provides a full list of affected products from Siemens Healthineers and provides recommendations to mitigate the vulnerabilities.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Aptio by Inpeco: All versions	Patch will be available after October 2019
Aptio by Siemens: All versions	Patch will be available after January 2020.
Atellica Data Manager: All versions	Customer bulletin CB 10810542 Rev. 94 will be released after August. 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
Atellica Process Manager: All versions	Customers using the Remote Control features with the RDP protocol are advised to follow the recommendations from the Microsoft advisory to patch the client and server systems.
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 1.21 available in Q4 of calendar year 2019.
CentraLink: All versions	Customer bulletin CB 10810542 Rev. 94 was released after August. 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

Iontris: VA11, VA12, VB11	Specific remediation actions for this product will be communicated to customers in direct letters.
MAGNETOM Vida, MAGNETOM Sola, MAGNETOM Lumina, MAGNETOM Altea, MAGNETOM Amira, and MAGNETOM Sempra: VA10A, VA10A-SP01, VA11A, VA11B, VA12M	• Users of VA10A need to upgrade to VA10A-SP01 or VA11B (where available) • Users of VA11A need to upgrade to VA11B • For VA10A-SP01, VA11B, and VA12M a security delivery (SD01) will be provided that closes port 3389 (scheduled for 10/2019) • The next regular version will contain the Microsoft patches.
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 Referal 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.
Somatom Go.Up, Somatom Go.Now, Somatom Go.Top, Somatom go.All: VA10A, VA20A	• Users of VA10A should upgrade to VA20A • Users of VA20A should install quarterly patches – VA20_SP3 will disable the RDP service and will close port 3389 (Scheduled for 09/2019) – VA20_SP4 will include the Microsoft patches

VM SIS Virtual Server, Sensis High End SIS Server: VD10B, VD11A, VD11B	Disable Remote Desktop Protocol (RDP) and Disable port 3389 from firewall exception. For all users of VD10B, VD11A versions: Upgrade to VD11B before applying Deja Blue Security Vulnerability Patch.
syngo Dynamics: 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 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 Virtual Cockpit: 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.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.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: All versions of receiver	• 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:

- Contact Siemens Healthineers Service Technician to obtain information if Remote Desktop Protocol (RDP) on the product can be disabled to mitigate the risk
- For Siemens Healthineers products that install on customer computers, customers are strongly recommended to secure those computers as soon as possible with the appropriate patches from Microsoft
- 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://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226

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.

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-2019-1181

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

Vulnerability CVE-2019-1182

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

Vulnerability CVE-2019-1222

An unauthenticated attacker with access to port 3389/tcp in an affected device may execute arbitrary commands with elevated privileges. This vulnerability only affects products based on Windows 10.

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

Vulnerability CVE-2019-1226

An unauthenticated attacker with access to port 3389/tcp in an affected device may execute arbitrary commands with elevated privileges.This vulnerability only affects products based on Windows 10.

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 (2019-09-10): Publication Date

TERMS OF USE