SSA-966341: SMBv1 Vulnerabilities in Molecular Diagnostics Products from Siemens Healthineers

Publication Date: 2017-05-17
Last Update: 2018-06-19
Current Version: V1.1
CVSS v3.0 Base Score: 9.8

SUMMARY

Select Molecular Diagnostics products from Siemens Healthineers are affected by the Microsoft Windows SMBv1 vulnerabilities. The exploitability of the vulnerabilities depends on the actual configuration and deployment environment of each product.

Siemens Healthineers has developed solutions for all affected products which are available via customer support. Siemens Healthineers also provides specific countermeasures for systems that have not yet been remediated.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Tissue Preparation System: All versions	Siemens Healthineers customer service engineers have been deploying fixes to affected systems since a solution was available. If in doubt, please contact your local Siemens Healthineers Customer Service Engineer, portal or Regional Support Center.
VERSANT kPCR Molecular System: All versions	Siemens Healthineers customer service engineers have been deploying fixes to affected systems since a solution was available. If in doubt, please contact your local Siemens Healthineers Customer Service Engineer, portal or Regional Support Center.
VERSANT kPCR Sample Prep: All versions	Siemens Healthineers customer service engineers have been deploying fixes to affected systems since a solution was available. If in doubt, please contact your local Siemens Healthineers Customer Service Engineer, portal or Regional Support Center.

WORKAROUNDS AND MITIGATIONS

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

- Until solutions can be applied by the customer support and for end-of-support products, Siemens Healthineers recommends to isolate affected products that are listening on network ports 139/tcp, 445/tcp or 3389/tcp from any infected system within its respective network segment (e.g. by firewall blocking access to above network ports).
- If the above cannot be implemented and patient safety and treatment is not at risk, disconnect the product from the network and use in standalone mode. Reconnect the product only after the

provided patch or remediation is installed on the system.

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

Molecular Diagnostics products from Siemens Healthineers are used for in vitro diagnostic testing in laboratory environments for the extraction of nucleic acids from a variety of clinical sample types using magnetic bead extraction technology, and, separately, for the automated amplification and detection of nucleic acids using kPCR (real time) technology.

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-2017-0143

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

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:H/RL:O/RC:C

Vulnerability CVE-2017-0144

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

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:H/RL:O/RC:C

Vulnerability CVE-2017-0145

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

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:H/RL:O/RC:C

Vulnerability CVE-2017-0146

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

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:H/RL:O/RC:C

Vulnerability CVE-2017-0147

An authenticated remote attacker could potentially disclose information from the server by sending specially crafted packets to the SMBv1 server of affected Microsoft Windows systems.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Vulnerability CVE-2017-0148

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

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:H/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 (2017-05-17): Publication Date
V1.1 (2018-06-19): New format; Added update 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.