SSA-286693: SMBv1 Vulnerabilities in Laboratory Diagnostics Products from Siemens Healthineers

Publication Date 2017-05-17
Last Update 2017-08-07
Current Version V1.2
CVSS v3.0 Base Score 9.8

SUMMARY

Select Laboratory 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

- Atellica® COAG 360: All versions
- BCS® XP: All versions
- BN ProSpec®: All versions
- Atellica NEPH 630: All versions
- BEP 2000 Advance®: All versions
- Quadriga BeFree: All versions
- ADVIA® 2120i: All versions
- ADVIA 120: All versions
- Sysmex® CS-2000i/2100i: All versions
- Sysmex CS-2500: All versions
- Sysmex CS-5100: All versions
- ADVIA 560: All versions
- ADVIA Chemistry 1800: All versions
- ADVIA Chemistry 2400: All versions
- ADVIA Chemistry XPT: All versions
- ADVIA Centaur® XP: All versions
- ADVIA Centaur CP: All versions
- ADVIA Centaur XPT: All versions
- Dimension Vista®: All versions
- IMMULITE® 1000: All versions
- IMMULITE 2000: All versions
- syngo® Laboratory Connectivity Manager: All versions
- syngo Laboratory Data Manager: All versions
- Aptio® Automation: All versions
- ADVIA Automation: All versions

- VersaCell®: All versions
- VersaCell X3: All versions
- Viva™: All versions

DESCRIPTION

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

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (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 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 2 (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 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 3 (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 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 4 (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 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 5 (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 Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Vulnerability 6 (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 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

SOLUTION

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.

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 we recommend the following:

- If patient safety and treatment is not at risk, disconnect the uninfected product from the network and use in standalone mode.
- Reconnect the product only after the provided patch or remediation is installed on the system.

In addition, Siemens Healthineers recommends to have appropriate backups and system restoration procedures in place.

ADDITIONAL RESOURCES

[1] Customer Information on WannaCry Malware for Siemens Healthineers Imaging and Diagnostics Products is available here:
https://www.siemens.com/cert/pool/cert/siemens_security_bulletin_ssb-412479.pdf

[2] For further inquiries on 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 (2017-05-22): Removed Dimension® from list of affected products
V1.2 (2017-08-07): Updated solution

DISCLAIMER