SSA-755010: Vulnerability in RAPIDLab 1200 and RAPIDPoint 400/500 Blood Gas Analyzers

Publication Date: 2018-06-12
Last Update: 2018-06-26
Current Version: V1.1
CVSS v3.0 Base Score: 8.8

SUMMARY

Siemens Healthineers has become aware of two potential cybersecurity vulnerabilities for the RAPIDLab® 1200 Series and RAPIDPoint® 400/405/500 Blood Gas Analyzers and recommends specific countermeasures to mitigate the risk.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RAPIDLab 1200 systems / RAPIDPoint 400 systems / RAPIDPoint 500 systems: All versions *without* use of Siemens Healthineers Informatics products	• Restrict physical access to only authorized individuals to limit exposure to CVE-2018-4845. • Disable Remote Viewing feature by following the instructions in the “Enabling or Disabling Remote Viewing” section of the analyzer Operator’s Guide to limit exposure to CVE-2018-4845 and mitigate CVE-2018-4846.
RAPIDLab 1200 Series: All versions < V3.3 *with* Siemens Healthineers Informatics products	• Restrict physical access to only authorized individuals to limit exposure to CVE-2018-4845. • Upgrade to V3.3 or 3.3.1. Please contact your Siemens Healthineers service desk for more information. • Change the password according to the release notes, or contact the service department. • To ensure seamless and secure connectivity with the RAPIDComm® Data Management System, RAPIDComm® V7.0 or higher is recommended.

RAPIDPoint 500 systems: All versions >= V3.0 *with* Siemens Healthineers Informatics products	• Restrict physical access to only authorized individuals to limit exposure to CVE-2018-4845. • Change the password according to the release notes or contact the service department. • To ensure seamless and secure connectivity with RAPIDComm, RAPIDComm V7.0 or higher is recommended.
RAPIDPoint 500 systems: V2.4.X *with* Siemens Healthineers Informatics products	• Restrict physical access to only authorized individuals to limit exposure to CVE-2018-4845. • Upgrade to and follow instructions provided for V3.0.
RAPIDPoint 500 systems: All versions =< V2.3 *with* Siemens Healthineers Informatics products	• Restrict physical access to only authorized individuals to limit exposure to CVE-2018-4845. • Siemens Healthineers will update this advisory when new information becomes available.
RAPIDPoint 400 systems: All versions *with* Siemens Healthineers Informatics products	• Restrict physical access to only authorized individuals to limit exposure to CVE-2018-4845. • Upgrade to RAPIDPoint 500 Series. • If upgrading is not an option, disable Remote Viewing feature by following the instructions in the “Enabling or Disabling Remote Viewing” section of the analyzer Operator’s Guide to limit exposure to CVE-2018-4845 and mitigate CVE-2018-4846.

WORKAROUNDS AND MITIGATIONS

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

- For specific mitigations or workarounds, please see table above.

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

The RAPIDLab 1200 system is a cartridge-based blood gas, electrolyte, and metabolite analyzer designed for use in medium- to high-volume clinical laboratories.

The RAPIDPoint 400/405/500 systems are cartridge-based analyzers for blood-gas, electrolytes, and metabolites designed for use in point-of-care environments.

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-2018-4845

Remote attackers with either local or remote credentialed access to the "Remote View" feature might be able to elevate their privileges, compromising confidentiality, integrity, and availability of the system. No special skills or user interaction are required to perform this attack. At the time of advisory publication, no public exploitation of this security vulnerability is known. Siemens Healthineers confirms the security vulnerability and provides mitigations to resolve the security issue.

CVSS v3.0 Base Score	8.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability CVE-2018-4846

A factory account with hardcoded password might allow attackers access to the device over port 5900/tcp. Successful exploitation requires no user interaction or privileges and impacts the confidentiality, integrity, and availability of the affected device. At the time of advisory publication, no public exploitation of this security vulnerability is known. Siemens Healthineers confirms the security vulnerability and provides mitigations to resolve the security issue.

CVSS v3.0 Base Score	7.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:T/RC:C

ACKNOWLEDGMENTS

Siemens Healthineers thanks the following parties for their efforts:

- Oran Avraham from MEDIGATE for coordinated disclosure

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 (2018-06-12): Publication Date

V1.1 (2018-06-26): Added acknowledgement

TERMS OF USE