



CVE-2018-4845

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 03/24/2023 05:32:00 PM UTC

CVE-2018-4845

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Rapidlab 1200](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in RAPIDLab 1200 systems / RAPIDPoint 400 systems / RAPIDPoint 500 systems (All versions _without_ use of Siemens Healthineers Informatics products), RAPIDLab 1200 Series (All versions < V3.3 _with_ Siemens Healthineers Informatics products), RAPIDPoint 500 systems (All versions >= V3.0 _with_ Siemens Healthineers Informatics products), RAPIDPoint 500 systems (V2.4.X _with_ Siemens Healthineers Informatics products), RAPIDPoint 500 systems (All versions =< V2.3 _with_ Siemens Healthineers Informatics products), RAPIDPoint 400 systems (All versions _with_ Siemens Healthineers Informatics products).

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.

CVE-2018-4845 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Third Party Advisory cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-755010.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Siemens	Rapidlab 1200	-	All	All	All
Hardware 	Siemens	Rapidlab 1200	-	All	All	All
Operating System	Siemens	Rapidlab 1200 Firmware	All	All	All	All
Operating System	Siemens	Rapidlab 1200 Firmware	All	All	All	All
Hardware 	Siemens	Rapidpoint 400	-	All	All	All
Hardware 	Siemens	Rapidpoint 400	-	All	All	All
Operating System	Siemens	Rapidpoint 400 Firmware	-	All	All	All
Operating System	Siemens	Rapidpoint 400 Firmware	-	All	All	All
Hardware 	Siemens	Rapidpoint 500	-	All	All	All
Hardware 	Siemens	Rapidpoint 500	-	All	All	All
Operating System	Siemens	Rapidpoint 500 Firmware	All	All	All	All
Operating System	Siemens	Rapidpoint 500 Firmware	All	All	All	All
Operating System	Siemens	Rapidpoint 500 Firmware	All	All	All	All

cpe:2.3:h:siemens:rapidlab_1200:-:*****:

cpe:2.3:h:siemens:rapidlab_1200:-:*****:

