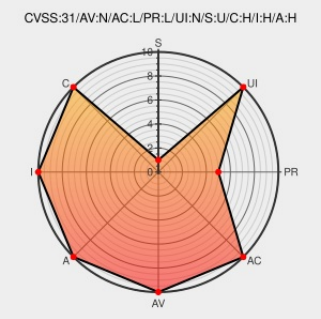
CVE-2022-43546

Published on: Not Yet Published

Last Modified on: 06/13/2023 09:15:00 AM UTC

CVE-2022-43546

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of 7kg9501-0aa01-2aa1 from Siemens contain the following vulnerability:

A vulnerability has been identified in POWER METER SICAM Q200 family (All versions < V2.70), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P850 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10), SICAM P855 (All versions < V3.10). Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.

CVE-2022-43546 has been assigned by 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

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-887249.pdf
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-570294.pdf
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-572005.pdf

Related QID Numbers

591244 Siemens SICAM Q100 Session Fixation, Improper Input Validation Multiple Vulnerabilities (ICSA-22-314-11, SSA-570294)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	7kg9501-0aa01-2aa1	-	All	All	All
Operating System	Siemens	7kg9501-0aa01-2aa1 Firmware	All	All	All	All
Hardware	Siemens	7kg9501-0aa31-2aa1	-	All	All	All
Operating System	Siemens	7kg9501-0aa31-2aa1 Firmware	All	All	All	All

cpe:2.3:h:siemens:7kg9501-0aa01-2aa1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:7kg9501-0aa01-2aa1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:7kg9501-0aa31-2aa1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:7kg9501-0aa31-2aa1_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-43546 : A vulnerability has been identified in POWER METER SICAM Q100 All versions < V2.50 , POWER METER… twitter.com/i/web/status/1…	2022-11-08 10:51:12
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-43546 A vulnerability has been identified in POWER METER SICAM Q100 (Al… twitter.com/i/web/status/1…	2022-11-08 11:56:00

/r/netcve	CVE-2022-43546	2022-11-08 11:38:47

← Previous ID

Next ID→