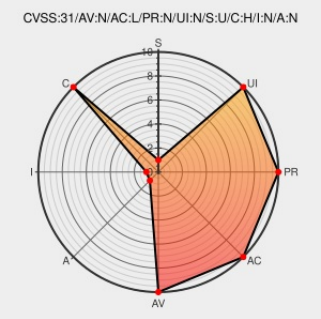
CVE-2021-46304

Published on: Not Yet Published

Last Modified on: 07/21/2023 04:52:00 PM UTC

CVE-2021-46304

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



Certain versions of Cp-8000 Master Module With I/o -25/ 70 from Siemens contain the following vulnerability:

A vulnerability has been identified in CP-8000 MASTER MODULE WITH I/O -25/+70°C (All versions), CP-8000 MASTER MODULE WITH I/O -40/+70°C (All versions), CP-8021 MASTER MODULE (All versions), CP-8022 MASTER MODULE WITH GPRS (All versions). The component allows to activate a web server module which provides unauthenticated access to its web pages. This could allow an attacker to retrieve debug-level information from the component such as internal network topology or connected systems.

CVE-2021-46304 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Siemens** - **CP-8000 MASTER MODULE WITH I/O -25/+70°C** version **All versions**

Affected Vendor/Software: **Siemens** - **CP-8000 MASTER MODULE WITH I/O -40/+70°C** version **All versions**

Affected Vendor/Software: **Siemens** - **CP-8021 MASTER MODULE** version **All versions**

Affected Vendor/Software: **Siemens** - **CP-8022 MASTER MODULE WITH GPRS** version **All versions**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	CONFIRM N/A

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.

Related QID Numbers

591287 Siemens SICAM A8000 Web Server Module Improper Access Control Vulnerability (ICSA-22-223-05, SSA-185638)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Cp-8000 Master Module With I/o -25/ 70	-	All	All	All
Operating System	Siemens	Cp-8000 Master Module With I/o -25/ 70 Firmware	All	All	All	All
Hardware	Siemens	Cp-8000 Master Module With I/o -40/ 70	-	All	All	All
Operating System	Siemens	Cp-8000 Master Module With I/o -40/ 70 Firmware	All	All	All	All
Hardware	Siemens	Cp-8021 Master Module	-	All	All	All
Operating System	Siemens	Cp-8021 Master Module Firmware	All	All	All	All
Hardware	Siemens	Cp-8022 Master Module With Gprs	-	All	All	All
Operating System	Siemens	Cp-8022 Master Module With Gprs Firmware	All	All	All	All

cpe:2.3:h:siemens:cp-8000_master_module_with_i\/o_-25\/\+70:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:cp-8000_master_module_with_i\/o_-25\/\+70_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:cp-8000_master_module_with_i\/o_-40\/\+70:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:cp-8000_master_module_with_i\/o_-40\/\+70_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:cp-8021_master_module:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:cp-8021_master_module_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:cp-8022_master_module_with_gprs:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:cp-8022_master_module_with_gprs_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-46304 : A vulnerability has been identified in CP-8000 MASTER MODULE WITH I/O -25/+70°C All versions , CP… twitter.com/i/web/status/1…	2022-08-10 11:22:52

@JohnJasonFallow	New vulnerability on the NVD: CVE-2021-46304 ift.tt/FSoMpg1	2022-08-10 14:11:13
/r/netcve	CVE-2021-46304	2022-08-10 12:38:49

← Previous ID

Next ID→