



CVE-2021-33720

Published on: 09/14/2021 12:00:00 AM UTC

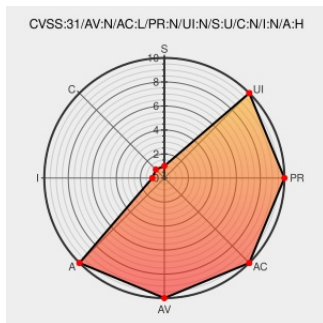
Last Modified on: 10/12/2021 10:15:00 AM UTC

CVE-2021-33720

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Siprotec 5 With Cpu Variant Cp050](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SIPROTEC 5 relays with CPU variants CP050 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP100 (All versions < V8.80), SIPROTEC 5 relays with CPU variants CP300 (All versions < V8.80). Specially crafted packets sent to port 4443/tcp could cause a Denial-of-Service condition.

CVE-2021-33720 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) Siemens - SIPROTEC 5 relays with CPU variants CP050 version All versions < V8.80

Affected Vendor/Software: [S](#) Siemens - SIPROTEC 5 relays with CPU variants CP100 version All versions < V8.80

Affected Vendor/Software: [S](#) Siemens - SIPROTEC 5 relays with CPU variants CP300 version All versions < V8.80

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	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	S MISC cert-portal.siemens.com/productcert/pdf/ssa-847986.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
Operating System	Siemens	Siprotec 5 With Cpu Variant Cp050	All	All	All	All
Operating System	Siemens	Siprotec 5 With Cpu Variant Cp100	All	All	All	All
Operating System	Siemens	Siprotec 5 With Cpu Variant Cp200	All	All	All	All
Operating System	Siemens	Siprotec 5 With Cpu Variant Cp300	All	All	All	All

`cpe:2.3:o:siemens:siprotec_5_with_cpu_variant_cp050:*:*:*:*:*:`

`cpe:2.3:o:siemens:siprotec_5_with_cpu_variant_cp100:*:*:*:*:*:`

`cpe:2.3:o:siemens:siprotec_5_with_cpu_variant_cp200:*:*:*:*:*:`

`cpe:2.3:o:siemens:siprotec_5_with_cpu_variant_cp300:*:*:*:*:*:`

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-33720 : A vulnerability has been identified in SIPROTEC 5 relays with CPU variants CP050 All versions < V... twitter.com/i/web/status/1...	2021-09-14 10:57:17

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 [Twitter](#) [LinkedIn](#) |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web](#)

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report