



CVE-2021-33737

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

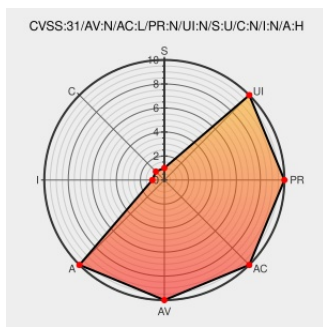
Last Modified on: 09/28/2021 03:38:00 PM UTC

CVE-2021-33737

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Simatic Cp343-1](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SIMATIC CP 343-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 343-1 Advanced (incl. SIPLUS variants) (All versions), SIMATIC CP 343-1 ERPC (All versions), SIMATIC CP 343-1 Lean (incl. SIPLUS variants) (All versions), SIMATIC CP 443-1 (incl. SIPLUS variants) (All versions), SIMATIC CP 443-1 Advanced (incl. SIPLUS variants) (All versions). Sending a specially crafted packet to port 102/tcp of an affected device could cause a Denial-of-Service condition. A restart is needed to restore normal operations.

CVE-2021-33737 has been assigned by [S productcert@siemens.com](mailto:productcert@siemens.com) to track the vulnerability - currently rated as **HIGH** severity.

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: **7.8 - HIGH**

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

CVE References

Description	Tags	Link
-------------	------	------

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	Simatic Cp343-1	-	All	All	All
Hardware	Siemens	Simatic Cp343-1 Advanced	-	All	All	All
Operating System	Siemens	Simatic Cp 343-1 Advanced Firmware	All	All	All	All
Hardware	Siemens	Simatic Cp 343-1 Erpc	All	All	All	All
Operating System	Siemens	Simatic Cp 343-1 Erpc Firmware	All	All	All	All
Operating System	Siemens	Simatic Cp 343-1 Firmware	All	All	All	All
Hardware	Siemens	Simatic Cp 343-1 Lean	All	All	All	All
Operating System	Siemens	Simatic Cp 343-1 Lean Firmware	All	All	All	All
Hardware	Siemens	Simatic Cp 443-1	All	All	All	All
Hardware	Siemens	Simatic Cp 443-1 Advanced	All	All	All	All
Operating System	Siemens	Simatic Cp 443-1 Advanced Firmware	All	All	All	All
Operating System	Siemens	Simatic Cp 443-1 Firmware	All	All	All	All

cpe:2.3:h:siemens:simatic_cp343-1:-:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_cp343-1_advanced:-:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cp_343-1_advanced_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_cp_343-1_erpc:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cp_343-1_erpc_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cp_343-1_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_cp_343-1_lean:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cp_343-1_lean_firmware:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_cp_443-1:*:*:*:*:*:*:


cpe:2.3:h:siemens:simatic_cp_443-1_advanced:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cp_443-1_advanced_firmware:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cp_443-1_firmware:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-33737 : A vulnerability has been identified in SIMATIC CP 343-1 incl. SIPLUS variants All versions , SI... twitter.com/i/web/status/1...	2021-09-14 10:57:45

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#)