



CVE-2020-25242

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-25242
State	PUBLIC
Assigner	productcert@siemens.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-12 14:15:00 UTC
Updated	2021-12-03 19:52:00 UTC
Description	A vulnerability has been identified in SIMATIC NET CP 343-1 Advanced (incl. SIPLUS variants) (All versions), SIMATIC NE

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Simatic Net Cp 343-1 Advanced	-	All	All	All
Operating System	Siemens	Simatic Net Cp 343-1 Advanced Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 343-1 Lean	-	All	All	All
Operating System	Siemens	Simatic Net Cp 343-1 Lean Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 343-1 Standard	-	All	All	All
Operating System	Siemens	Simatic Net Cp 343-1 Standard Firmware	All	All	All	All

References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/pdf/ssa-676775.pdf	MISC	cert-portal.siemens.com	
Siemens SIMATIC NET CP343-1 CISA	MISC	us-cert.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)