

CVE-2016-8562

Siemens SIMATIC CP 1543-1 Improper Privilege Management Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

A vulnerability has been identified in SIMATIC CP 1543-1 (All versions < V2.0.28), SIPLUS NET CP 1543-1 (All versions < V2.0.28). Under special conditions it was possible to write SNMP variables on port 161/udp which should be read-only and should only be configured with TIA-Portal. A write to these variables could reduce the availability or cause a denial-of-service.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.036 89.4th percentile · FIRST	CISA DEADLINE Mar 24, 2022 KEV since 2022 · listed over a year
---	---------------------------------------	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.036 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
simatic cp 1543-1 firmware	< 2.0.28	2.0.28	NVD
siplus net cp 1543-1 firmware	< 2.0.28	2.0.28	NVD
simatic cp 1543-1	—	no fixed version listed	NVD
siplus net cp 1543-1	—	no fixed version listed	NVD

Sources

Vendor guidance	cert-portal.siemens.com/productcert/pdf/ssa-672373.pdf	NVD	nvd.nist.gov/vuln/detail/CVE-2016-8562
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-9410
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-8562		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.