



CVE-2017-6868

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

Summary

CVE	CVE-2017-6868
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-07 17:29:00 UTC
Updated	2017-12-30 02:29:00 UTC
Description	An Improper Authentication issue was discovered in Siemens SIMATIC CP 44x-1 RNA, all versions prior to 1.4.1. An unaut

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Simatic Cp 44x-1 Redundant Network Access Modules	All	All	All	All

References

Reference	Source	Link
Siemens	CONFIRM	www.siemens.com
Siemens SIMATIC CP 44x-1 Redundant CVE-2017-6868 Authentication Bypass Vulnerability	BID	www.securityfocus.com/bid/98888
Siemens SIMATIC CP 44x-1 RNA Unspecified Bug Lets Remote Users Gain Elevated Privileges - SecurityTracker	SECTrack	www.securitytracker.com/id/1038888
Siemens SIMATIC CP 44x-1 Redundant Network Access Modules ICS-CERT	MISC	ics-cert.us-cert.gov/ICS-CERT-17-008
CVE Program record	CVE.ORG	www.cve.org/CVE.expanded/CVE@2017-07-07
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2017-6868

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

591064 Siemens SIMATIC CP 44x-1 Redundant Network Access Modules Vulnerability (ICSA-17-173-01) (SSA-126840)

© [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](#)