



CVE-2016-7112

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-7112
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-06 00:59:00 UTC
Updated	2018-03-23 01:29:00 UTC
Description	A vulnerability has been identified in Firmware variant PROFINET IO for EN100 Ethernet module : All versions < V1.04.01;

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	En100 Ethernet Module	-	All	All	All
Hardware	Siemens	En100 Ethernet Module	-	All	All	All
Application	Siemens	En100 Ethernet Module Firmware	All	All	All	All

References

Reference	Source	Link	Tag
Siemens EN100 Ethernet Modules for Reyrolle ICSA-17-187-02 Multiple Security Vulnerabilities	BID	www.securityfocus.com	
Siemens EN100 Ethernet Module CVE-2016-7112 Authentication Bypass Vulnerability	BID	www.securityfocus.com	
Siemens	CONFIRM	www.siemens.com	
Siemens SIPROTEC 4 and SIPROTEC Compact (Update F) CISA	MISC	ics-cert.us-cert.gov	
Siemens	CONFIRM	www.siemens.com	Ven
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

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