



CVE-2015-1601

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

Summary

CVE	CVE-2015-1601
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-06 01:59:00 UTC
Updated	2016-11-28 19:18:00 UTC
Description	Siemens SIMATIC STEP 7 (TIA Portal) 12 and 13 before 13 SP1 Upd1 allows man-in-the-middle attackers to obtain sensi

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Simatic Step 7	12	All	All	All
Application	Siemens	Simatic Step 7	13	All	All	All
Application	Siemens	Simatic Step 7	12	All	All	All
Application	Siemens	Simatic Step 7	13	All	All	All
Application	Siemens	Simatic Step 7	All	sp1	All	All

References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/pdf/ssa-487246.pdf	CONFIRM	cert-portal.siemens.com	
Siemens	CONFIRM	www.siemens.com	Patch,
Siemens SIMATIC STEP 7 TIA Portal Man in the Middle Information Disclosure Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

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](#).

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