



CVE-2016-7165

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

Summary

CVE	CVE-2016-7165
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-15 19:30:00 UTC
Updated	2018-06-15 01:29:00 UTC
Description	A vulnerability has been identified in Primary Setup Tool (PST) (All versions < V4.2 HF1), SIMATIC IT Production Suite (All

Risk And Classification

Problem Types: CWE-254 | CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Primary Setup Tool	-	All	All	All
Application	Siemens	Primary Setup Tool	-	All	All	All
Application	Siemens	Security Configuration Tool	-	All	All	All
Application	Siemens	Security Configuration Tool	-	All	All	All
Application	Siemens	Simatic It Production Suite	-	All	All	All
Application	Siemens	Simatic It Production Suite	-	All	All	All
Application	Siemens	Simatic Net Pc Software	All	All	All	All
Application	Siemens	Simatic Pcs7	8.0	All	All	All
Application	Siemens	Simatic Pcs7	8.1	All	All	All
Application	Siemens	Simatic Pcs7	8.2	All	All	All
Application	Siemens	Simatic Pcs7	8.0	All	All	All
Application	Siemens	Simatic Pcs7	8.1	All	All	All
Application	Siemens	Simatic Pcs7	8.2	All	All	All
Application	Siemens	Simatic Pcs 7	All	All	All	All
Application	Siemens	Simatic Step 7	All	sp4	All	All
Application	Siemens	Simatic Step 7 Tia Portal	All	All	All	All
Application	Siemens	Simatic Step 7 Tia Portal	All	All	All	All

Application	Siemens	Simatic Winac Rtx 2010	-	All	All	All
Application	Siemens	Simatic Winac Rtx 2010	-	All	All	All
Application	Siemens	Simatic Winac Rtx F 2010	-	All	All	All
Application	Siemens	Simatic Winac Rtx F 2010	-	All	All	All
Application	Siemens	Simatic Wincc	7.0	sp3	All	All
Application	Siemens	Simatic Wincc	7.2	All	All	All
Application	Siemens	Simatic Wincc	7.3	All	All	All
Application	Siemens	Simatic Wincc	7.4	All	All	All
Application	Siemens	Simatic Wincc	7.0	sp3	All	All
Application	Siemens	Simatic Wincc	7.2	All	All	All
Application	Siemens	Simatic Wincc	7.3	All	All	All
Application	Siemens	Simatic Wincc	7.4	All	All	All
Application	Siemens	Simatic Wincc	All	sp2	All	All
Application	Siemens	Simatic Wincc Tia Portal	-	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	All	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	All	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	All	All	All	All
Application	Siemens	Simatic Wincc Runtime	-	All	All	All
Application	Siemens	Simatic Wincc Runtime	-	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	-	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	-	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	All	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	All	All	All	All
Application	Siemens	Simatic Wincc Tia Portal	All	All	All	All
Application	Siemens	Simit	9.0	All	All	All
Application	Siemens	Simit	9.0	All	All	All
Application	Siemens	Sinema Remote Connect	-	All	All	All
Application	Siemens	Sinema Remote Connect	-	All	All	All
Application	Siemens	Sinema Server	All	sp2	All	All
Application	Siemens	Softnet Security Client	All	All	All	All
Application	Siemens	Telecontrol Basic	All	sp2	All	All

References

Reference	Source	Link	Tags
Multiple Siemens Products CVE-2016-7165 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com	Third P

cert-portal.siemens.com/productcert/pdt/ssa-/01/08.pdt	CONFIRM	cert-portal.siemens.com	
Siemens Industrial Products Local Privilege Escalation Vulnerability (Update A) ICS-CERT	MISC	ics-cert.us-cert.gov	Third P
CVE-2016-7165 Privilege Escalation flaw affects many Siemens solutionsSecurity Affairs	MISC	securityaffairs.co	Third P
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report