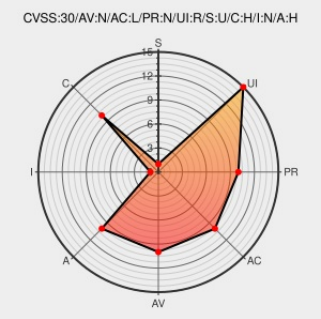
CVE-2016-9160

Published on: 12/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9160

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Simatic Pcs 7 from Siemens contain the following vulnerability:

A vulnerability in SIEMENS SIMATIC WinCC (All versions < SIMATIC WinCC V7.2) and SIEMENS SIMATIC PCS 7 (All versions < SIMATIC PCS 7 V8.0 SP1) could allow a remote attacker to crash an ActiveX component or leak parts of the application memory if a user is tricked into clicking on a malicious link under certain conditions.

CVE-2016-9160 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	HIGH

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
Siemens SIMATIC WinCC and SIMATIC PCS 7 ActiveX Vulnerability | ICS-CERT	ics-cert.us-cert.gov text/html	MISC ics-cert.us-cert.gov/advisories/ICSA-16-348-04
SIMATIC WinCC and SIMATIC PCS 7 CVE-	cve report (archive)	BID 94825

2016-9160 ActiveX Control Security Bypass Vulnerability	text/html	
Siemens SIMATIC WinCC ActiveX Flaw Lets Remote Users Obtain Potentially Sensitive Information or Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1037435
Siemens	www.siemens.com application/pdf	CONFIRM www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-693129.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Simatic Pcs 7	All	All	All	All
Application	Siemens	Simatic Wincc	All	All	All	All

cpe:2.3:a:siemens:simatic_pcs_7:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→