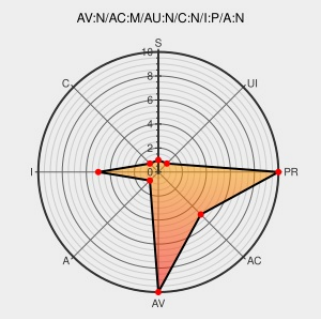
CVE-2012-3031

Published on: 09/18/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:16 PM UTC

CVE-2012-3031

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



Certain versions of Simatic Pcs7 from Siemens contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in WebNavigator in Siemens WinCC 7.0 SP3 and earlier, as used in SIMATIC PCS7 and other products, allow remote attackers to inject arbitrary web script or HTML via a (1) GET parameter, (2) POST parameter, or (3) Referer HTTP header.

CVE-2012-3031 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
404 - File Not Found | CISA	US Government Resource, www.us-cert.gov, application/pdf, Inactive Link, Not Archived	MISC www.us-cert.gov/control_systems/pdf/ICSA-12-256-01.pdf
Vulnerabilities	web.archive.org, text/html, Inactive Link, Not Archived	MISC en.securitylab.ru/lab/PT-2012-42
Siemens	Patch, Vendor Advisory, www.siemens.com, application/pdf	CONFIRM www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-864051.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 Pcs7	8.0	All	All	All
Application	Siemens	Simatic Pcs7	8.0	All	All	All
Application	Siemens	Wincc	5.0	All	All	All
Application	Siemens	Wincc	5.0	sp1	All	All
Application	Siemens	Wincc	6.0	All	All	All
Application	Siemens	Wincc	6.0	sp2	All	All
Application	Siemens	Wincc	6.0	sp3	All	All
Application	Siemens	Wincc	6.0	sp4	All	All
Application	Siemens	Wincc	7.0	All	All	All
Application	Siemens	Wincc	7.0	sp1	All	All
Application	Siemens	Wincc	7.0	sp2	All	All
Application	Siemens	Wincc	5.0	All	All	All
Application	Siemens	Wincc	5.0	sp1	All	All
Application	Siemens	Wincc	6.0	All	All	All
Application	Siemens	Wincc	6.0	sp2	All	All
Application	Siemens	Wincc	6.0	sp3	All	All
Application	Siemens	Wincc	6.0	sp4	All	All
Application	Siemens	Wincc	7.0	All	All	All
Application	Siemens	Wincc	7.0	sp1	All	All
Application	Siemens	Wincc	7.0	sp2	All	All
Application	Siemens	Wincc	All	sp3	All	All

cpe:2.3:a:siemens:simatic_pcs7:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_pcs7:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:5.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:5.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:6.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:siemens:wincc:*:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→