



CVE-2013-0676

Published on: 03/21/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:39 PM UTC

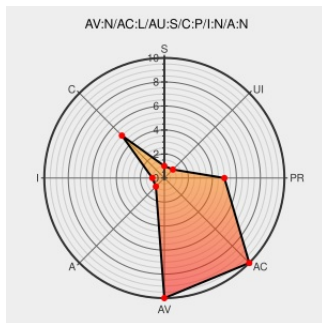
CVE-2013-0676

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Simatic Pcs7](#) from [Siemens](#) contain the following vulnerability:

Siemens WinCC before 7.2, as used in SIMATIC PCS7 before 8.0 SP1 and other products, does not properly assign privileges for the database containing WebNavigator credentials, which allows remote authenticated users to obtain sensitive information via a SQL query.

CVE-2013-0676 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Siemens

[Vendor Advisory](#)
www.siemens.com
[text/html](#)

S CONFIRM www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-714398.pdf

Siemens WinCC 7.0 SP3 Multiple
Vulnerabilities | ICS-CERT

[US Government Resource](#)
web.archive.org
[text/html](#)
Inactive Link **Not Archived**

MISC ics-cert.us-cert.gov/pdf/ICSA-13-079-02.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	7.1	sp3	All	All
Application	Siemens	Simatic Pcs7	7.1	sp3	All	All
Application	Siemens	Simatic Pcs7	All	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	7.0	sp3	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	7.0	sp3	All	All
Application	Siemens	Wincc	All	All	All	All

```
cpe:2.3:a:siemens:simatic_pcs7:7.1:sp3:*:*:*:*:
```

```
cpe:2.3:a:siemens:simatic_pcs7:7.1:sp3:*:*:*:*:
```

```
cpe:2.3:a:siemens:simatic_pcs7:*:*:*:*:*:*:
```

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)