SSA-345843: Vulnerabilities in WinCC 7.2

Publication Date: 2013-06-14
Last Update: 2013-06-24
Current Version: V1.1
CVSS Overall Score: 5.9

Summary:
WinCC Web Navigator is susceptible to three vulnerabilities which could be exploited over the network. The first vulnerability is a SQL injection vulnerability which compromises the confidentiality, integrity and availability of the affected system. The remaining two vulnerabilities are located in the Web Navigator login and session management. If attackers exploit such vulnerabilities they could circumvent the authentication or guess user names.

Siemens provides an update which fixes these vulnerabilities.

AFFECTED PRODUCTS
The following product versions are affected:
- WinCC 7.2 and earlier
- SIMATIC PCS7 V8.0 SP1 and earlier

DESCRIPTION
The Web Navigator component of WinCC gives users the possibility to control their plants via web browser with the same look-and-feel as local operator stations. This Web Navigator application is vulnerable to three different vulnerabilities. Attackers might access the Web Navigator web application as authenticated user or perform read and write operations on the database of the WinCC SQL database.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION
The vulnerability classification has been performed by using the CVSSv2 scoring system (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2013-3957)
Attackers might overcome the input filtering of the WinCC Web Navigator login screen and inject SQL statements into queries. By manipulating the database, the attacker can elevate his rights and, depending on the system configuration, might be able to gain full system access.

- CVSS Base Score: 7.5
- CVSS Temporal Score: 5.9
- CVSS Overall Score: 5.9 (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2013-3958)
Hard coded credentials are used in the Web Navigator login mechanism. Attackers with network access and knowledge of the credentials could log into the Web Navigator web applications as authenticated user.

- CVSS Base Score: 7.5
- CVSS Temporal Score: 5.9
- CVSS Overall Score: 5.9 (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)
Vulnerability 3 (CVE-2013-3959)

A user with authenticated access to the Web Navigator web application can probe for valid NetBIOS user names by manipulating URL parameters.

CVSS Base Score 4.0
CVSS Temporal Score 3.1
CVSS Overall Score 3.1 (AV:N/AC:L/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Mitigating factors:
The first two vulnerabilities can only be exploited if the attacker has network access to the Web Navigator web interface.

SOLUTION

Siemens provides WinCC 7.2 Update 1 [1], which fixes the described vulnerabilities for both affected products. Siemens recommends installing the update as soon as possible.

Note: Users of SIMATIC PCS7 with an earlier version as V8.0 SP1 must upgrade to this version first, and then install WinCC 7.2 Update 1.

As a further mitigation measure Siemens strongly recommends to protect the network access to the Web Navigator web interface with appropriate mechanism.

In general, Siemens strongly recommends to protect systems according to recommended security practices [4] and to configure the environment according to operational guidelines [2] in order to run the affected software components in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Alexander Tlyapov, Sergey Gordeychik and Timur Yunusov from Positive Technologies for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

1. The patch can be obtained here: http://support.automation.siemens.com/WW/view/en/73443294
4. Recommended security practices by US-CERT: http://ics-cert.us-cert.gov/content/recommended-practices
5. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2013-06-14): Publication Date
V1.1 (2013-06-24): Updated Acknowledgement Section and Additional Resources

DISCLAIMER

See: http://www.siemens.com/terms_of_use