

SSA-214365: Vulnerabilities in SIMATIC WinCC

Publication Date 2014-07-23
Last Update 2014-10-07
Current Version V1.1
CVSS Overall Score 5.3

Summary:

The latest software release of SIMATIC WinCC fixes several vulnerabilities. The most severe of these vulnerabilities could allow privilege escalation in the WinCC Project administration application under certain conditions. The attacker must have network access to the WinCC server to exploit this vulnerability.

All vulnerabilities resolved with this software release are discussed below.

AFFECTED PRODUCTS

- SIMATIC WinCC: all versions < V7.3
- SIMATIC PCS7 (as WinCC is incorporated): all versions < V8.1

DESCRIPTION

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system. It is used to monitor and control physical processes involved in industry and infrastructure on a large scale and over long distances.

Five vulnerabilities have been resolved in WinCC V7.3. 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-2014-4682)

The SIMATIC WinCC WebNavigator server at port 80/tcp and port 443/tcp could allow unauthenticated access to sensitive data if specially crafted HTTP requests are sent to this port.

CVSS Base Score 5.0
CVSS Temporal Score 3.9
CVSS Overall Score 3.9 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2014-4683)

Existent access control of the WinCC WebNavigator server at port 80/tcp and port 443/tcp could allow remote authenticated users to escalate their privileges in WinCC.

CVSS Base Score 4.9
CVSS Temporal Score 3.8
CVSS Overall Score 3.8 (AV:N/AC:M/Au:S/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 3 (CVE-2014-4684)

The database server of SIMATIC WinCC could allow authenticated users to escalate their privileges in the database if a specially crafted command is sent to the database server at port 1433/tcp.

CVSS Base Score 6.0
CVSS Temporal Score 4.7
CVSS Overall Score 4.7 (AV:N/AC:M/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 4 (CVE-2014-4685)

Access permissions on system objects could allow a local user to obtain limited escalated privileges within the operating system.

CVSS Base Score 4.6
CVSS Temporal Score 3.6
CVSS Overall Score 3.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 5 (CVE-2014-4686)

A hard coded encryption key could allow privilege escalation in the WinCC Project administration application if its network communication on port 1030/tcp of a legitimate user can be captured.

CVSS Base Score 6.8
CVSS Temporal Score 5.3
CVSS Overall Score 5.3 (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Mitigating factors:

For vulnerabilities 2 and 3 authenticated access is required.

For vulnerabilities 4 an attacker must have local access to the system.

All other vulnerabilities require network access to the corresponding port.

SOLUTION

Siemens has released SIMATIC WinCC V7.3 [1,2] and SIMATIC PCS7 V8.1 [3] which fix these vulnerabilities and recommends upgrading as soon as possible.

Until the updates can be deployed, Siemens advises to apply the following steps to mitigate the risk:

- Limit the WebNavigator server access to trusted networks/clients only
- Ensure that the WebNavigator clients authenticate themselves against the WebNavigator server (e.g. use client certificates)
- Restrict access to the WinCC database server at port 1433/tcp to trusted entities
- Deactivate all unnecessary OS users on WinCC server
- Run WinCC server and engineering stations within a trusted network, or
- Ensure that the WinCC server and the engineering stations communicate via encrypted channels only (e.g. establish a VPN tunnel)

SIMATIC WinCC V7.3 introduces the feature "Encrypted Communications". The feature allows operators to add an extra layer of security to protect the server's communication. Siemens strongly recommends activating this feature.

As a general security measure Siemens strongly recommends to protect network access to the SIMATIC WinCC server with appropriate mechanisms. It is also advised to follow recommended security practices [6] and to configure the environment according to operational guidelines [4] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Sergey Gordeychik, Alexander Tlyapov, Dmitry Nagibin, and Gleb Gritsai from Positive Technologies for coordinated disclosure of vulnerabilities 1, 2, 4, and 5.

ADDITIONAL RESOURCES

- [1] Detailed information on the new SIMATIC WinCC version:
<http://support.automation.siemens.com/WW/view/en/97493192>
- [2] The new software version can be ordered via the Industry Mall website:
<https://mall.industry.siemens.com/mall/de/de/Catalog/Products/10042373?tree=CatalogTree>
- [3] Detailed information on the new SIMATIC PCS7 version:
<http://support.automation.siemens.com/WW/view/en/98161292>
- [4] An overview of the recommended operational guidelines for Industrial Security (with the cell protection concept):
http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
- [5] Information about Industrial Security published by Siemens:
<http://www.siemens.com/industrialsecurity>
- [6] Recommended security practices published by ICS-CERT:
<http://ics-cert.us-cert.gov/content/recommended-practices>
- [7] 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 (2014-07-23): Publication Date
- V1.1 (2014-10-07): Added fix for SIMATIC PCS7

DISCLAIMER

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