SSA-134508: Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC in TIA Portal

Publication Date 2014-11-21
Last Update 2014-12-11
Current Version V1.2
CVSS Overall Score 8.3

Summary:

The latest software update for SIMATIC WinCC fixes two critical vulnerabilities. One could allow unauthenticated remote code execution.

Siemens has released software updates for WinCC, PCS 7 and TIA Portal. Siemens is working on updates for further versions of the affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS

- SIMATIC WinCC:
  - V7.0 SP3 and earlier versions
  - V7.2: All versions < V7.2 Update 9
  - V7.3: All versions < V7.3 Update 2
- SIMATIC PCS 7 (as WinCC is incorporated):
  - V7.1 SP4 and earlier versions
  - V8.0: All versions < V8.0 SP2 with WinCC V7.2 Update 9
  - V8.1: All versions with WinCC V7.3 < Update 2
- TIA Portal V13 (including WinCC Professional Runtime): All versions < V13 Update 6

DESCRIPTION

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system, PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, and TIA Portal is an engineering software for SIMATIC products.

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-2014-8551)

A component within WinCC could allow remote code execution for unauthenticated users if specially crafted packets are sent to the WinCC server.

CVSS Base Score 10.0
CVSS Temporal Score 8.3
CVSS Overall Score 8.3 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

Vulnerability 2 (CVE-2014-8552)

A component within WinCC could allow unauthenticated users to extract arbitrary files from the WinCC server if specially crafted packets are sent to the server.

CVSS Base Score	7.8
CVSS Temporal Score	6.1
CVSS Overall Score	6.1 (AV:N/AC:L/Au:N/C:C/I:N/A:N/E:POC/RL:OF/RC:C)

Mitigating factors

The attacker must have network access to the affected system.

SOLUTION

Siemens has released updates for the following products and strongly encourages customers to upgrade to the new versions as soon as possible:

- WinCC V7.0: Upgrade to WinCC V7.0 SP2 Update 11 [6]
- WinCC V7.2: Upgrade to WinCC V7.2 Update 9 [2]
- WinCC V7.3: Upgrade to WinCC V7.3 Update 2 [3]
- PCS 7 V8.0 SP2:
  - Upgrade to WinCC V7.2 Update 9 [2]
  - Upgrade to OpenPCS 7 V8.0 SP1 Update 5 [4]
  - Upgrade to Route Control V8.0 SP1 Update 4 [4]
  - Upgrade to BATCH V8.0 SP1 Update 11 [4]
- PCS 7 V8.1:
  - Upgrade to WinCC V7.3 Update 2 [3]
  - Upgrade to OpenPCS 7 V8.1 Update 1 [5]
  - Upgrade to Route Control V8.1 Update 1 [5]
  - Upgrade to BATCH V8.1 Update 1 [5]
- TIA Portal V13 (including WinCC Professional Runtime): Upgrade to WinCC V13 Update 6 [1]

Siemens is preparing updates for WinCC V7.0 SP3 and PCS 7 V7.1 SP4 with OpenPCS 7, Route Control or BATCH which will fix the vulnerabilities. As soon as new releases become available, Siemens will update this advisory.

In the meantime, customers should mitigate the risk of their products by implementing the following steps:

- Always run WinCC server and engineering stations within a trusted network
- Ensure that the WinCC server and the engineering stations communicate via encrypted channels only (e.g. activate feature “Encrypted Communications” in WinCC V7.3 (PCS 7 V8.1), or establish a VPN tunnel)
- Restrict access to the WinCC server to trusted entities
- Apply up-to-date application whitelisting software and virus scanners

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 [9] and to configure the environment according to operational guidelines [7] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and coordination efforts:

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- Symantec Deepsight Intelligence

ADDITIONAL RESOURCES

[1] Updates for WinCC Runtime Professional V13:
http://support.automation.siemens.com/WW/view/en/90527654

[2] Update 9 for WinCC 7.2:
http://support.automation.siemens.com/WW/view/en/104151435

[3] Update 2 for WinCC 7.3:
http://support.automation.siemens.com/WW/view/en/105898606

[4] Updates for PCS 7 V8.0 SP2:
http://support.automation.siemens.com/WW/view/en/106224418

[5] Updates for PCS 7 V8.1:
http://support.automation.siemens.com/WW/view/en/106226042

[6] Update 11 for WinCC 7.0 SP2
http://support.automation.siemens.com/WW/view/en/107174184

[7] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

[8] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

[9] Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

[10] 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 (2014-11-21): Publication Date
V1.1 (2014-11-28): Added updates for PCS 7 V8.0 SP2
V1.2 (2014-12-11): Added updates for PCS 7 V8.1 and WinCC 7.0 SP2

DISCLAIMER