SSA-378531: Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC Runtime Professional

Publication Date 2016-07-22
Last Update 2016-11-07
Current Version V1.3
CVSS v3.0 Base Score 9.8

SUMMARY

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

Siemens has released updates for all affected products.

AFFECTED PRODUCTS

- SIMATIC WinCC:
  - V7.0 SP2 and earlier: All versions < V7.0 SP2 Update 12
  - V7.0 SP3: All versions < V7.0 SP3 Update 8
  - V7.2: All versions < V7.2 Update 13
  - V7.3: All versions < V7.3 Update 10
  - V7.4: All versions < V7.4 Update 1
- SIMATIC PCS 7 (WinCC, BATCH, Route Control, OpenPCS 7)
  - V7.1 SP4 and earlier versions < V7.1 SP4 with WinCC V7.0 SP2 Update 12
  - V8.0: All versions < V8.0 SP2 with WinCC V7.2 Update 13
  - V8.1: All versions < V8.1 SP1 with WinCC V7.3 Update 10
  - V8.2: All versions < V8.2 with WinCC V7.4 Update 1
- SIMATIC WinCC Runtime Professional: All versions < V13 SP1 Update 9

DESCRIPTION

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system. SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC. SIMATIC WinCC Runtime Professional is a human machine interface (HMI).

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSS v3.0) (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-2016-5743)

Specially crafted packets sent to SIMATIC WinCC or WinCC Runtime Professional could allow remote code execution for unauthenticated users.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2016-5744)

Specially crafted packets sent to SIMATIC WinCC could allow unauthenticated users to extract arbitrary files from the WinCC station. This vulnerability only affects WinCC V7.0 and WinCC V7.2.

CVSS Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/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:

- SIMATIC WinCC V7.0 SP2 and earlier: Update to V7.0 SP2 Update 12 [1]
- SIMATIC WinCC V7.0 SP3: Update to V7.0 SP3 Update 8 [2]
- SIMATIC WinCC V7.2: Update to WinCC V7.2 Update 13 [3]
- SIMATIC WinCC V7.3: Update to WinCC V7.3 Update 10 [4]
- SIMATIC WinCC V7.4: Update to WinCC V7.4 Update 1 [5]
- SIMATIC PCS 7 V7.1 SP4 and earlier versions:
  - WinCC: Update to WinCC V7.0 SP2 Update 12 [1]
  - BATCH: Update to BATCH V7.1 SP1 Update 21 [6]
  - BATCH: Update to BATCH V7.1 SP2 Update 11 [6]
  - Route Control: Update to Route Control V7.1 SP2 Update 6 [6]
  - OpenPCS 7: Update to OpenPCS 7 V7.1 SP4 Update 2 [6]
- SIMATIC PCS 7 V8.0 SP2:
  - WinCC: Update to WinCC V7.2 Update 13 [3]
  - BATCH: Update to BATCH V8.0 SP1 Update 17 [7]
  - Route Control: Update to Route Control V8.0 SP1 Update 6 [7]
  - OpenPCS 7: Update to OpenPCS 7 V8.0 SP1 Update 8 [7]
- SIMATIC PCS 7 V8.1 SP1:
  - WinCC: Update to WinCC V7.3 Update 10 [4]
  - BATCH: Update to BATCH V8.1 SP1 Update 11 [8]
  - Route Control: Update to Route Control V8.1 Update 2 [8]
  - OpenPCS 7: Update to OpenPCS 7 V8.1 Update 3 [8]
- SIMATIC PCS 7 V8.2:
  - WinCC: Update to WinCC V7.4 Update 1 [5]
  - BATCH: Update to BATCH V8.2 Update 1 [9]
  - Route Control: Update to Route Control V8.2 Update 1 [9]
  - OpenPCS 7: Update to OpenPCS7 V8.2 Update 1 [9]
- SIMATIC WinCC Runtime Professional V13: Update to WinCC Runtime Professional V13 SP1 Update 9 [10]

Until the updates can be applied, Siemens recommends the following steps to mitigate the risk:

- Always run WinCC, WinCC Runtime Professional and PCS 7 stations within a trusted network
- Ensure that WinCC, WinCC Runtime Professional and PCS 7 stations communicate via encrypted channels only (e.g. activate feature “Encrypted Communications” in WinCC V7.3 and PCS 7 V8.1 SP1, or establish a VPN tunnel)
- Restrict access to the WinCC, WinCC Runtime Professional and PCS 7 stations 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 and SIMATIC PCS 7 stations with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [11] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Sergey Temnikov and Vladimir Dashchenko, Critical Infrastructure Defence Team, Kaspersky Lab for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

[1] Update 12 for WinCC V7.0 SP2:
https://support.industry.siemens.com/cs/ww/en/view/109741519

[2] Update 8 for WinCC V7.0 SP3:
https://support.industry.siemens.com/cs/ww/en/view/109741127

[3] Update 13 for WinCC V7.2:
https://support.industry.siemens.com/cs/ww/en/view/109739416

[4] Update 10 for WinCC V7.3:
https://support.industry.siemens.com/cs/ww/en/view/109738470

[5] Update 1 for WinCC V7.4:
https://support.industry.siemens.com/cs/ww/en/view/109738653

[6] Updates for PCS V7.1 SP4:
https://support.industry.siemens.com/cs/ww/en/view/109738681

[7] Updates for PCS V8.0 SP2:
https://support.industry.siemens.com/cs/ww/en/view/109738680

[8] Updates for PCS 7 V8.1 SP1:
https://support.industry.siemens.com/cs/ww/en/view/109738678

[9] Updates for PCS 7 V8.2:
https://support.industry.siemens.com/cs/ww/en/view/109738674

[10] Updates for WinCC Runtime Professional V13:
https://support.industry.siemens.com/cs/ww/en/view/109311724

[11] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[12] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[13] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-07-22):	Publication Date
V1.1 (2016-08-11):	Added fix information for WinCC V7.2, Route Control and SIMATIC BATCH V8.2
V1.2 (2016-09-27):	Added fix information for WinCC V7.0 SP2, WinCC V7.0 SP3, PCS 7 V7.1 SP4 (WinCC and Route Control), and PCS 7 V8.0 (WinCC, BATCH, Open PCS 7)
V1.3 (2016-11-07):	Corrected fix information for PCS 7 V8.0 and V8.1; Added fix information for PCS 7 V8.0 (Route Control) and PCS 7 V7.1 (OpenPCS 7 and BATCH);

DISCLAIMER