SSA-342587: Vulnerabilities in SIMATIC WinCC Open Architecture

Publication Date	2014-02-03
Last Update	2014-03-20
Current Version	V1.1
CVSS Overall Score	7.3

Summary:

Multiple potential vulnerabilities were identified within SIMATIC WinCC OA which might allow attackers to either escalate their privileges, to traverse through the file system of the WinCC OA server, to perform Denial of Service attacks or remote code execution over the network.

Siemens provides software updates which fix these vulnerabilities.

AFFECTED PRODUCTS

- SIMATIC WinCC OA all versions < 3.12 P002 January

DESCRIPTION

The client-server HMI (human machine interface) system SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

Four potential vulnerabilities were identified within SIMATIC WinCC OA which might allow attackers to either escalate their privileges, to traverse through the file system of the WinCC OA server, to perform Denial of Service attacks or remote code execution over the network.

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-2014-1696)

Attackers might be able to break project users' password hashes and escalate their privileges within the affected WinCC OA server application.

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-2014-1697)

The integrated web server at port 4999/tcp might allow attackers to perform remote code execution by sending specially crafted packets over the network without authentication.

CVSS Base Score	9.3
CVSS Temporal Score	7.3
CVSS Overall Score	7.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C)

Vulnerability 3 (CVE-2014-1698)

The integrated web server at port 4999/tcp might allow attackers to traverse through the file system of the server based on the application's Windows user permissions by sending specially crafted packets over the network without authentication.

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 4 (CVE-2014-1699)

Malformed HTTP requests sent over the network without authentication to the web server's port 4999/tcp might lead to a Denial of Service of the SIMATIC WinCC OA monitoring service. Restarting the WinCC OA Console recovers the monitoring service.

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

Mitigating factors:

The attacker must have network access to the affected devices to be able to exploit the above vulnerabilities.

SOLUTION

The following software updates fix the potential vulnerabilities:

- SIMATIC WinCC OA v3.12 [1]: vulnerabilities 1, 3, 4
- SIMATIC WinCC OA v3.12 P002 January [2]: vulnerability 2

Siemens recommends updating to SIMATIC WinCC OA v3.12 and to install patch P002 January.

Further, for secure operation of SIMATIC WINCC Open Architecture Siemens strongly recommends configuring SIMATIC WinCC OA according to its security concept [3].

As a general security measure Siemens strongly recommends to protect network access to the SIMATIC WinCC Open Architecture server with appropriate mechanisms. It is 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 the following for their support and efforts:

- Gleb Gritsai, Ilya Karpov and Kirill Nesterov from Positive Technologies for coordinated disclosure of the vulnerabilities

ADDITIONAL RESOURCES

[1] The version update can be obtained here:
https://portal.etm.at/index.php?option=com_phocadownload&view=category&id=12:versions&Itemid=81

[2] The patch can be obtained here:
https://portal.etm.at/index.php?option=com_phocadownload&view=category&id=2:pvss-patches&Itemid=81

[3] The WinCC OA security concept can be obtained here:
https://portal.etm.at/index.php?option=com_phocadownload&view=category&download=910:wincc_oa-security-concept-v3.12&id=52:security&Itemid=81

[4] An overview of the 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 by Siemens:
http://www.siemens.com/industrialsecurity

[6] Recommended security practices 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 (2014-02-03): Publication Date

V1.1 (2014-03-20): Added Information for WinCC OA Security Concept

DISCLAIMER