SSA-714398: Vulnerabilities in WinCC 7.0 SP3 Update 1

Publication Date 2013-03-15
Last Update 2013-03-15
Current Version V1.0
CVSS Overall Score 5.3

Summary:

WinCC stores Windows user credentials (user names and passwords) in a database. Authenticated users can log into this database, break the existing obfuscation and extract passwords.

Furthermore, the database permissions allowed unprivileged users to gain access to sensitive data.

A third vulnerability was found in the WinCC web server, where authenticated users could browse the file system via URL manipulation and extract sensitive information.

A fourth vulnerability was found in the ActiveX component “RegReader”, which is vulnerable to a buffer overflow and possible remote code execution.

Manipulated project files can trigger a fifth vulnerability, which can allow an attacker to take over the WinCC PC.

Furthermore a communication component called CCEServer is vulnerable to a remote buffer overflow that can be triggered over the network.

Siemens has released a new software version that fixes the above mentioned vulnerabilities.

AFFECTED PRODUCTS

- WinCC 7.0 SP3 Update1 and below
- As WinCC is part of SIMATIC PCS7, the SIMATIC PCS 7 Web Server is also affected by these vulnerabilities

DESCRIPTION

For managing authentication and authorization, WinCC stores user passwords for WebNavigator in an MS SQL database. If an attacker can successfully log into the WinCC database server, these passwords can be extracted. In the database the passwords are obfuscated, but the obfuscation can be removed without too much effort.

Moreover, too many rights were given to several users in the database. The need-to-know principle was not followed strictly, so users with low privilege could read e.g. password fields. This vulnerability could become relevant if combined with the first finding.

These two vulnerabilities can be exploited locally and remotely, but valid credentials are needed to access the database.

The third vulnerability is often called “arbitrary file reading”, “forceful browsing” or “directory traversal”. The WinCC web server might return sensitive data if certain file names and paths are queried, e.g. via URL parameters. However, the user needs to be authenticated on the web server to exploit this vulnerability.

The fourth vulnerability is a buffer overflow in an ActiveX component called “RegReader”. For using certain WinCC functionality, the user has to install this component in his web browser. If the user visits a malicious web site, this web site might also call and execute RegReader. As RegReader does not check properly the length of parameters, the malicious site can trigger a buffer overflow with possible remote code execution in the context of the user’s browser.

The fifth vulnerability is caused by insecure parsing of project files. If a legitimate user opens a manipulated project, sensitive data can be transmitted via the network or a DoS condition can be provoked.

The last vulnerability is a buffer overflow in a central communication component of WinCC. Attackers with access to the network might exploit this vulnerability and trigger a Denial-of-Service against WinCC.

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

WebNavigator passwords stored in the SQL database are only obfuscated.

CVSS Base Score	2.7
CVSS Temporal Score	2.1
CVSS Overall Score	2.1 (AV:A/AC:L/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2

Users with legitimate, non-privileged access to WinCC's MS SQL database can retrieve obfuscated user passwords for WebNavigator. For doing this, access to the system is needed either locally or from the adjacent network and the user's account must have adequate permissions.

CVSS Base Score	2.7
CVSS Temporal Score	2.1
CVSS Overall Score	2.1 (AV:A/AC:L/Au:S/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 3

Authenticated users may manipulate the URL in the web browser to access the file system of the web server. With this vulnerability they may read all the files that are readable in the web server context.

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)

Vulnerability 4

An ActiveX control "RegReader" which is installed in the user's web browser is susceptible to a buffer overflow. An attacker might trick a victim into visiting a malicious web site which calls this ActiveX control, triggers the overflow and take over the victim's PC.

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)

Vulnerability 5

By opening a manipulated project file, sensitive data can be transmitted over the network or a DoS condition can be provoked.

CVSS Base Score	5.8
CVSS Temporal Score	4.5
CVSS Overall Score	4.5 (AV:N/AC:M/Au:N/C:P/I:N/A:P/E:POC/RL:OF/RC:C)

Vulnerability 6

By sending a specially crafted packet to a dynamically assigned port, an attacker can generate a DoS condition against WinCC.

CVSS Base Score	6.1
CVSS Temporal Score	5.0
CVSS Overall Score	5.0 (AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C)

Mitigating factors:

For vulnerabilities 1 and 2, the attacker must have a legitimate access to the system where WinCC's database is located.

For exploiting vulnerability 3, the attacker must be authenticated at the web server.

Vulnerability 4 requires social engineering and the user must use the same browser for internal and external web pages.

Vulnerability 5 requires social engineering. For transmitting data over the network, the attacker's host must be reachable from the engineering station.

Vulnerability 6 can only be exploited if the attacker has access to the vulnerable port.

SOLUTION

Siemens has fixed these issues in WinCC 7.2. This version can be ordered on the customer support web site [1].

This WinCC 7.2 version is also part of SIMATIC PCS7 V8.0 SP 1.

ACKNOWLEDGEMENT

Siemens thanks Gleb Gritsai, Sergey Gordeychik from Positive Technologies for coordinated disclosure of findings 1-5.

ADDITIONAL RESOURCES

1. https://eb.automation.siemens.com/mall/de/de/Catalog/Products/10042373?tree=CatalogTree
2. 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
3. Information about Industrial Security by Siemens: http://www.siemens.com/industrialsecurity
4. Recommended security practices by US-CERT: http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
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 (2013-03-15): Publication Date

DISCLAIMER