SSA-212483: Vulnerabilities in WinCC (TIA Portal) V11

Publication Date 2013-03-15
Last Update 2013-03-15
Current Version V1.0
CVSS Overall Score 3.6

Summary:

This advisory treats seven different vulnerabilities that have been found in the software running on SIMATIC HMIs that are engineered with WinCC (TIA Portal) V11, partially impacting confidentiality, integrity and availability of the system.

The vulnerabilities affect the web server of engineered HMIs and their internal password management. Possible attacks require either physical access to the HMI or an authenticated user, so an attacker must either have valid user credentials or must use social engineering on a legitimate user.

When the vulnerabilities are exploited they allow password retrieval, web session hijacking, source code retrieval, display of false data and Denial-of-Service.

Siemens addresses these issues by a new software version.

AFFECTED PRODUCTS

SIMATIC HMIs managed with the following software:

- WinCC (TIA Portal) V11 (all versions)

DESCRIPTION

The vulnerabilities affect the HMI's web server and the internal password store. Possible attacks require either physical access to the HMI or an authenticated user, so an attacker must either have valid user credentials or must use social engineering on a legitimate user. Additionally the web server of the system must be enabled for the web-based vulnerabilities.

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-2011-4515)

User credentials for the HMI's web application are stored within the HMI's system. This data is obfuscated in a reversible way and is readable and writable for users with physical access or Sm@rt Server access to the 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 2

By manipulating HTTP requests an authenticated attacker may crash the HMI's web application. The web application will become unavailable until the device is restarted.

CVSS Base Score	4.0
CVSS Temporal Score	3.1
CVSS Overall Score	3.1 (AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Vulnerability 3

The HMI's web application is susceptible to stored Cross-Site-Scripting attacks. An authenticated user may store data on the web application which will execute malicious JavaScript when the affected page is accessed by other users.

CVSS Base Score	4.0
CVSS Temporal Score	3.1
CVSS Overall Score	3.1 (AV:N/AC:L/Au:S/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 4

By manipulating the URL an authenticated attacker may have access to source code of the panel's server-side web application files, which may include user defined scripts.

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 5

If a user clicks on a malicious link which seems to lead to a HMI web application, it is possible to display any data to the user (HTTP response splitting).

CVSS Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 6

If a user clicks on a malicious link which seems to lead to a HMI web application, it is possible to display any data to the user (server-side script injection).

CVSS Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 7

The HMI's web application is susceptible to reflected Cross-Site-Scripting attacks. If a legitimate user clicks on a malicious link, JavaScript code may get executed and session information may be stolen.

CVSS Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating factors:

For vulnerabilities 1-4, an attacker must have authenticated access to the web application. For vulnerabilities 5-7, an authenticated user must be tricked into opening a malicious URL. Furthermore, the web server must be manually enabled on the HMIs to exploit the web-related vulnerabilities, as it is disabled by default.

SOLUTION

All vulnerabilities are fixed in the new software version WinCC (TIA Portal) V12. As a workaround to close the web-based vulnerabilities, the HMI's web server may be disabled.

Siemens recommends operating the devices only within trusted networks [3].

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Billy Rios, Terry McCorkle and Shawn Merdinger for coordinated disclosure of vulnerability 1.
- Gleb Gritsai, Sergey Bobrov, Roman Ilin, Artem Chaykin, Timur Yunusov, Ilya Karpov from Positive Technologies for coordinated disclosure of all seven vulnerabilities.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts.

ADDITIONAL RESOURCES

1. Information about WinCC V12:
   http://support.automation.siemens.com/WW/view/en/67797516
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