SSA-345442: Multiple Vulnerabilities in WinCC flexible and WinCC V11 (TIA Portal)

Publishing Date 2012-01-24
Last Update 2012-01-24
Current Version V1.5
CVSS Overall Score 8.7

Summary:

Multiple vulnerabilities have been reported in the products WinCC flexible and WinCC V11 (TIA Portal). Siemens AG will address the vulnerabilities by software fixes and documentation updates.

AFFECTED SOFTWARE

- WinCC flexible versions 2004, 2005, 2007, 2008
- WinCC V11 (TIA portal)
- Multiple SIMATIC HMI panels (TP, OP, MP, Comfort Panels, Mobile Panels)
- WinCC V11 Runtime Advanced
- WinCC flexible Runtime

The following related products are **not** affected:

- WinCC V11 (TIA Portal) Basic
- WinCC V11 (TIA Portal) Runtime Professional
- WinCC V6.x and V7.x

DESCRIPTION

Three components within the affected software products were determined to contain vulnerabilities. In the following, each of the three components will be described.

There are multiple vulnerabilities in the web server that is contained in SIMATIC HMI panels and PC-based HMI devices configured with WinCC flexible and WinCC V11 (TIA Portal). This web server can be activated in the engineering system by the following runtime options:

- WinCC flexible: “HTML pages”, “Web service (SOAP)”, “SIMATIC HMI HTTP server”, “OPC server”
- WinCC V11 (TIA Portal): “HTML pages”, “HTTP channel server“, “Web service SOAP“, “Operate as OPC server“

When the web server is activated, it allows data retrieval and administration of the corresponding HMI device. It may contain vulnerabilities in the following areas:

- Weak web server authentication token generation
- Weak default passwords
- Cross-site scripting
- Possible header injection
- Directory traversal attack
- Denial-of-Service through URL manipulation
- Insufficient validation of project files

A detailed description of the vulnerabilities is located below, where the vulnerable web server is termed as “HMI web server”.

The Telnet service is provided by the operating system of the following SIMATIC HMI panels:

- Comfort Panels
- MP177, MP270, MP277, MP370, MP377
- OP177B, OP270, OP277
- TP177B, TP177B 4", TP270, TP277
- Mobile Panel 177, Mobile Panel 277, Mobile Panel 277 IWLAN (V1 and V2)

This service allows remote device access but does not offer authentication capabilities.

Multiple vulnerabilities were disclosed in the runtime loader of WinCC flexible and WinCC V11 (TIA Portal). When the transfer mode is activated for the device's Ethernet interface, the runtime loader listens on TCP port 2308 or, alternatively, on TCP port 50523. However, it does not sanitize its inputs sufficiently before processing them. If malicious data is sent to the port, an attacker may enforce a memory corruption leading to potential code execution or a denial of service.

Detailed information about the respective 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-2011-4508)

The HMI web server (see Section "Description") performs insecure authentication token generation for web sessions.

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 2 (CVE-2011-4509)

The HMI web server has a weak default password.

CVSS Base Score	10
CVSS Temporal Score	8.7
CVSS Overall Score	8.7 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Vulnerability 3 (CVE-2011-4510)

The HMI web server (see Section "Description") contains a cross-site scripting bug.

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 4 (CVE-2011-4511)

The HMI web server (see Section "Description") contains a further cross-site scripting bug.

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 5 (CVE-2011-4512)

The HMI web server (see Section "Description") is vulnerable to header 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 6 (CVE-2011-4513)

A vulnerability in the HMI web server and runtime loader (see Section “Description”) may allow an attacker to execute arbitrary code via specially crafted project files.

CVSS Base Score	10.0
CVSS Temporal Score	7.8
CVSS Overall Score	7.8 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C)

Vulnerability 7 (CVE-2011-4514)

The Telnet service (see Section “Description”) does not offer any capabilities for authentication.

CVSS Base Score	10
CVSS Temporal Score	8.7
CVSS Overall Score	8.7 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Vulnerability 8 (CVE-2011-4875)

With activated transfer mode, the runtime loader (see Section “Description”) does not properly validate the length of data segments and Unicode strings. This vulnerability may lead to remote code execution.

CVSS Base Score	9.3
CVSS Temporal Score	8.4
CVSS Overall Score	8.4 (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:POC/RL:U/RC:C)

Vulnerability 9 (CVE-2011-4876)

With activated transfer mode, the runtime loader (see Section “Description”) does not properly validate incoming strings and allows full access (read, write and execute) to any file within the file system.

CVSS Base Score	9.3
CVSS Temporal Score	8.4
CVSS Overall Score	8.4 (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:POC/RL:U/RC:C)

Vulnerability 10 (CVE-2011-4877)

With activated transfer mode, the runtime loader (see Section “Description”) does not sufficiently validate incoming data. Multiple vulnerabilities allow a Denial-of-Service attack which leads to a program crash.

CVSS Base Score	7.1
CVSS Temporal Score	6.4
CVSS Overall Score	6.4 (AV:N/AC:M/Au:N/C:N/I:N/A:C/E:POC/RL:U/RC:C)

Vulnerability 11 (CVE-2011-4878)

The HMI web server (see Section “Description”) does not properly validate URLs within HTTP requests. By manipulating URLs with encoded backslashes, directory traversal is possible. This leads to read access for all files within the file system.

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)

Vulnerability 12 (CVE-2011-4879)

The HMI web server (see Section “Description”) does not properly validate HTTP requests. By manipulating the first byte within URLs, the server switches to a special interpretation of the URL. This allows an attacker to read the application process memory and perform a Denial-of-Service attack by specifying invalid memory locations.

CVSS Base Score	8.5
CVSS Temporal Score	6.7
CVSS Overall Score	6.7 (AV:N/AC:L/Au:N/C:P/I:N/A:C/E:POC/RL:OF/RC:C)

Mitigating factors for vulnerabilities 1-6, 11 and 12 (HMI web server):

The HMI web server must be activated, and the attacker must have access to the network where the HMI web server is located and be able to access the relevant ports. If ports 80 and 443 of the affected systems are blocked, these vulnerabilities cannot be exploited.

Siemens recommends that the default password of the web server should always be changed as soon as possible.

Mitigating factors for vulnerability 7:

The Telnet service of the device must be activated, and the attacker must have access to the network where the Telnet daemon is located and be able to access the relevant port. If TCP port 23 of the affected systems is blocked, this vulnerability cannot be exploited.

All users of a WinCC flexible version below 2008 SP3 may deactivate the Telnet service as described in [5]. The Telnet service is deactivated by default in product versions WinCC flexible 2008 SP3 and above, as well as WinCC V11 (TIA Portal) SP2 and above.

Mitigating factors for vulnerabilities 8-10:

The transfer mode of the device must be activated, and the attacker must have access to the network where the HMI device is located and be able to access the relevant ports. If TCP ports 2308 and 50523 of the affected systems are blocked, these vulnerabilities cannot be exploited.

Siemens recommends deactivating the transfer mode after configuration of the device, as the transfer mode provides full access to the device [4], [6]. The transfer mode was implemented under the assumption that the device runs in a protected industrial environment.

SOLUTION

Siemens provides multiple measures for fixing the vulnerabilities:

Vulnerabilities 1, 3-5, 11, 12 (HMI web server):

The fixes for the reported vulnerabilities will be addressed by software updates WinCC V11 (TIA Portal) SP2 Update 1 and WinCC flexible 2008 SP3 [1]. Siemens strongly recommends installing the updates as soon as possible.

Vulnerability 2 (HMI web server):

This issue has been addressed by updating the product documentation contained in WinCC V11 (TIA Portal) SP2 Update 1 and WinCC flexible 2008 SP3 [1]. The updates provide a guide for the user and describe how to set a proper password for the service. Siemens strongly recommends that this guide is followed as soon as possible.

Vulnerability 6, 8-10 (HMI web server and runtime loader):

Deactivate the transfer mode of the device as described in user manuals. Siemens strongly recommends to protect systems according to recommended security practices [2], [3] and to configure the environment according to the operational guidelines.

Vulnerability 7 (Telnet service):

Deactivate the Telnet service as described in Section “Mitigating factors for vulnerability 7”. As Telnet is a clear text protocol, customers are advised to be aware of

risks when using the service. Therefore, it is recommended that network security mechanisms as mentioned in [2], [3] and [4] are implemented.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Billy Rios, Terry McCorkle, Shawn Merdinger and Luigi Auriemma for discovering the issues and for cooperating with us.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting the vulnerability and coordination efforts.

ADDITIONAL RESOURCES

1. The mentioned vulnerabilities will be addressed by the following software updates:
    a. WinCC flexible 2008 SP3:
    http://support.automation.siemens.com/WW/view/en/57267466
    b. WinCC V11 (TIA Portal) SP2 Update 1:
    http://support.automation.siemens.com/WW/view/en/58112582
    http://support.automation.siemens.com/WW/view/en/58112587
2. Recommended security practices by US-CERT:
    http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
3. Industrial Security home page:
    http://www.siemens.com/industrialsecurity
4. Operational Guidelines for Industrial Security
    http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/industrial_security_operational_guidelines_en.pdf
5. FAQ entry for disabling the Telnet service
    http://support.automation.siemens.com/WW/view/en/24460721
6. FAQ entry for configuration of Runtime Loader
    http://support.automation.siemens.com/WW/view/en/29054992
7. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
    http://www.siemens.com/cert

HISTORY DATA

V1.5 (2012-01-24): Official advisory publication

DISCLAIMER