ICS-CERT ADVISORY

ICSA-12-030-01A—SIEMENS SIMATIC WINCC MULTIPLE VULNERABILITIES

UPDATE A

April 18, 2012

OVERVIEW

This advisory is a follow-up to a previous advisory titled "ICSA-11-356-01 – Siemens HMI Authentication Vulnerabilities" that was published December 22, 2011, on the ICS-CERT web page[a] and an alert titled "ICS-ALERT-11-332-02A – Siemens SIMATIC WinCC Flexible Vulnerabilities" that was published December 2, 2011, on the ICS-CERT web page.[b]

ICS-CERT has received reports from independent security researchers Billy Rios, Terry McCorkle, Shawn Merdinger, and Luigi Auriemma detailing several vulnerabilities in Siemens SIMATIC WinCC Human-Machine Interface (HMI) application. ICS-CERT has coordinated with these researchers and Siemens to validate these vulnerabilities and include mitigation strategies in the latest Siemens service packs.[c]

AFFECTED PRODUCTS

According to Siemens, the following software packages are vulnerable:

- 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.

a. http://www.uscert.gov/control_systems/pdf/ICSA-11-356-01.pdf website last accessed April 16, 2012.
b. http://www.uscert.gov/control_systems/pdf/ICS-ALERT-11-332-02A.pdf website last accessed April 16, 2012.
c. Siemens ProductCERT advisories, http://www.siemens.com/cert/advisories/ website last accessed April 16, 2012.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to log on to a vulnerable system as a user or administrator with the ability to execute arbitrary code or obtain full access to files on the system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Siemens SIMATIC HMI is a software package used as an interface between the operator and the programmable logic controllers (PLCs) controlling the process. SIMATIC HMI performs the following tasks: process visualization, operator control of the process, alarm display, process value and alarm archiving, and machine parameter management. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical.

VULNERABILITY CHARACTERIZATION

VULNERABILITIES OVERVIEW

INSECURE AUTHENTICATION TOKEN GENERATION[d]

When a user (or administrator) logs on, the application sets predictable authentication token/cookie values. This can allow an attacker to bypass authentication checks and escalate privileges.

CVE-2011-4508[e] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0[f] calculator rates a CVSS Base Score of 9.3.

WEAK DEFAULT PASSWORDS[g]

The default administrator password is weak and easily brute forced. Siemens has changed the documentation to encourage users to change the password at first login.

CVE-2011-4509[h] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 10.0.

d. CWE-287: Improper Authentication, http://cwe.mitre.org/data/definitions/287.html, website last accessed April 16, 2012.
e. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4508 website last accessed April 16, 2012.
f. NVD Common Vulnerability Scoring System Support v2, http://nvd.nist.gov/cvss.cfm, website last accessed April 16, 2012.
g. CWE-255: Credentials Management, http://cwe.mitre.org/data/definitions/255.html, website last accessed April 16, 2012.
h. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4509, website last accessed April 16, 2012.

CROSS-SITE SCRIPTING VULNERABILITIES[i]

SIMATIC HMI Smart Options web server is vulnerable to two separate cross-site scripting attacks that may allow elevation of privileges, data theft, or service disruption.

CVE-2011-4510[j] and CVE-2011-4511[k] have been assigned to these vulnerabilities. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 4.3.

HEADER INJECTION VULNERABILITY[l]

The HMI web server is vulnerable to header injection that may allow elevation of privileges, data theft, or service disruption.

CVE-2011-4512[m] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 4.3.

CLIENT–SIDE ATTACK VIA SPECIALLY CRAFTED FILES[n]

This vulnerability can allow an attacker to execute arbitrary code via specially crafted project files. This may require social engineering to get the operator to download the files and execute them.

CVE-2011-4513[o] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 10.0.

LACK OF TELNET DAEMON AUTHENTICATION[p]

SIMATIC panels include a telnet daemon by default; however, the daemon does not include any authentication functions.

CVE-2011-4514[q] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 10.0.

i. CWE-79: Cross-site Scripting, http://cwe.mitre.org/data/definitions/79.html, website last accessed April 16, 2012.
j. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4510,. website last accessed April 16, 2012.
k. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4511, website last accessed April 16, 2012.
l. CWE-94: Code Injection, http://cwe.mitre.org/data/definitions/94.html, website last accessed April 16, 2012.
m. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4512, website last accessed April 16, 2012.
n. CWE-20: Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, website last accessed April 16, 2012.
o. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4513, website last accessed April 16, 2012.
p. CWE-255: Credentials Management, http://cwe.mitre.org/data/definitions/255.html, website last accessed April 16, 2012.
q. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4514 , website last accessed April 16, 2012.

STRING STACK OVERFLOW[r]

The runtime loader listens on Ports 2308/TCP or 50523/TCP while transfer mode is activated but does not properly validate the length of data segments and Unicode strings, which may cause a stack overflow. This vulnerability may lead to remote code execution.

CVE-2011-4875[s] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 9.3.

DIRECTORY TRAVERSAL[t]

The runtime loader listens on Ports 2308/TCP or 50523/TCP while transfer mode is activated but does not properly validate incoming strings. This allows an attacker full access (read, write, and execute) to any file within the file system.

CVE-2011-4876[u] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 9.3.

DENIALS OF SERVICE[v]

The runtime loader listens on Ports 2308/TCP or 50523/TCP while transfer mode is activated but does not sufficiently validate incoming data. Multiple vulnerabilities allow a denial-of-service (DoS) attack, which leads to a program crash.

CVE-2011-4877[w] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 7.1.

DIRECTORY TRAVERSAL[x]

The HMI web server does not properly validate URLs within HTTP requests on Ports 80/TCP and 443/TCP. By manipulating URLs with encoded backslashes, directory traversal is possible. This allows an attacker read access for all files within the file system.

CVE-2011-4878[y] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 7.8.

r. CWE-134: Uncontrolled Format String, http://cwe.mitre.org/data/definitions/134.html, website last accessed April 16, 2012.
s. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4875, website last accessed April 16, 2012.
t. CWE-22: Path Traversal, http://cwe.mitre.org/data/definitions/22.html, website last accessed April 16, 2012.
u. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4876, website last accessed April 16, 2012.
v. CWE-399: Resource Management Errors, http://cwe.mitre.org/data/definitions/399.html, website last accessed April 16, 2012.
w. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4877, website last accessed April 16, 2012.
x. CWE-22: Path Traversal, http://cwe.mitre.org/data/definitions/22.html, website last accessed April 16, 2012.
y. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4878, website last accessed April 16, 2012.

ARBITRARY MEMORY READ ACCESS[z]

The HMI web server does not properly validate HTTP requests. By manipulating the first byte within a URL, the server switches to a special interpretation of the URL. This allows an attacker to read the application process memory and perform a DoS attack by specifying invalid memory locations.

CVE-2011-4879[aa] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSS Version 2.0 calculator rates a CVSS Base Score of 8.5.

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker would need user interaction to exploit vulnerability #5.

The remaining vulnerabilities can be exploited remotely.

EXISTENCE OF EXPLOIT

Publicly available exploits are known to specifically target vulnerabilities #1, #2, and #7 through #11.

No known publicly available exploits specifically target vulnerabilities #3 through #6.

DIFFICULTY

These vulnerabilities would be very simple for a skilled attacker to exploit.

Exploiting vulnerability #5 requires social engineering to convince the user to accept and load the malformed file. This decreases the likelihood of a successful exploit.

MITIGATION

Each of the reported vulnerabilities has been addressed by Siemens, as follows:

- Insecure authentication token generation (#1), cross-site scripting (#3), header injection vulnerability (#4), HMI web server directory traversal (#10), and arbitrary memory read access vulnerabilities (#11).
  - Patches are included in Siemens' WinCC V11 (TIA Portal) SP2 Update 1[bb,cc] and WinCC flexible 2008 SP3.[dd]

z. CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, http://cwe.mitre.org/data/definitions/119.html, website last accessed April 16, 2012.

aa. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4879. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

bb. WinCC V11 (TIA Portal) SP2 Update 1, http://support.automation.siemens.com/WW/view/en/58112582 website last accessed April 16, 2012.

- Weak default passwords (#2).
  - Product documentation contained in WinCC V11 (TIA Portal) SP2 Update 1, and WinCC flexible 2008 SP3 has been updated to tell the user how to set a proper password during initial setup.
- Client-side attack via specially crafted files (#5), runtime loader string stack overflow (#7), runtime loader directory traversal (#8), runtime loader DoS (#9).
  - Siemens recommends that users deactivate the transfer mode after device configuration, because the transport mode provides full access to the device.[ee] The transport mode was implemented under the assumption that the software would be running in a protected industrial environment. Siemens strongly recommends that users protect systems according to recommended security practices[ff,gg] and configure the environment according to the operational guidelines.

--------- Begin Update A Part 1 of 1 --------

- Lack of telnet daemon authentication (#6).
  - Because telnet is a clear text protocol, customers are advised to be aware of corresponding risks. The telnet daemon is disabled by default in product versions WinCC flexible 2008 SP3 and newer, as well as WinCC V11 (TIA Portal) SP2 and newer. Siemens recommends disabling the telnet function on SIMATIC panels when telnet is not actively being used.

ICS-CERT tested WinCC V11 (TIA Portal) SP2 Update 1[hh,ii] and WinCC flexible 2008 SP3[jj] and found that it successfully resolves the following vulnerabilities:

- Insecure authentication token generation (#1)
- Cross-site scripting (#3)
- Header injection vulnerability (#4)
- HMI web server directory traversal (#10)
- Arbitrary memory read access vulnerabilities (#11).

cc. WinCC V11 (TIA Portal) SP2 Update 1, http://support.automation.siemens.com/WW/view/en/58112587 website last accessed April 16, 2012

dd. WinCC flexible 2008 SP3,http://support.automation.siemens.com/WW/view/en/57267466 website last accessed April 16, 2012

ee. Siemens Industry online support, http://support.automation.siemens.com/WW/view/en/29054992 website last accessed April 16, 2012.

ff. Siemens Operational Guidelines for Industrial Security, v1.1, http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/industrial_security_operational_guidelines_en.pdf website last accessed April 16, 2012.

gg. Siemens Industrial Security homepage, http://www.siemens.com/industrialsecurity website last accessed April 16, 2012.

hh. WinCC V11 (TIA Portal) SP2 Update 1, http://support.automation.siemens.com/WW/view/en/58112582 website last accessed April 16, 2012.

ii. WinCC V11 (TIA Portal) SP2 Update 1, http://support.automation.siemens.com/WW/view/en/58112587 website last accessed April 16, 2012.

jj. WinCC flexible 2008 SP3, http://support.automation.siemens.com/WW/view/en/57267466 website last accessed April 16, 2012.

The remaining vulnerabilities are addressed in documentation and a new FAQ[kk] entry on Siemens website. If unable to implement these changes, product users should contact their integrator or Siemens product support for assistance.

--------- End Update A Part 1 of 1 ----------

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[ll] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams* [mm] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[nn] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

[kk] Siemens FAQ, http://support.automation.siemens.com/WW/view/en/29054992, website last accessed April 16, 2012.
ll. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 16, 2012.
mm. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed April 16, 2012.
nn. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed April 16, 2012.

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.