ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-079-02—SIEMENS WINCC 7.0 SP3 MULTIPLE VULNERABILITIES

March 20, 2013

OVERVIEW

This advisory provides mitigation details for vulnerabilities that impact the Siemens SIMATIC WinCC.

Independent researcher Sergey Gordeychik of Positive Technologies and Siemens ProductCERT have identified multiple vulnerabilities[a] in the Siemens SIMATIC WinCC, which is used to configure SIMATIC operator devices. Siemens has produced a software update that fully resolves these vulnerabilities. Exploitation of these vulnerabilities could allow a denial-of-service (DoS) condition, unauthorized read access to files, or remote code execution. This could affect multiple industries, including food and beverage, water and wastewater, oil and gas, and chemical sectors worldwide.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following Siemens products are affected:

- WinCC 7.0 SP3 Update1 and below.

a. SSA-714398, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-714398.pdf, Web site last accessed March 20, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Note: As WinCC is part of SIMATIC PCS7, the SIMATIC PCS 7 Web Server is also affected by these vulnerabilities.

IMPACT

Successful exploitation of these vulnerabilities may result in a DoS condition, unauthorized read access to files, or remote code execution.

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 in the software package impacting multiple sectors worldwide.

BACKGROUND

Siemens is a multinational company headquartered in Munich, Germany. Siemens develops products mainly in the energy, transportation, and healthcare sectors.

SIMATIC WinCC is a software package used as an interface between the operator and the programmable logic controllers (PLCs). SIMATIC WinCC 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

VULNERABILITY OVERVIEW

MISSING ENCRYPTION OF SENSITIVE DATA[b]

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. This would allow an attacker access to all functions and privileges of all WinCC users.

CVE-2013-0678[c] has been assigned to this vulnerability. A CVSS v2 base score of 6.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:P/A:P).[d]

b. CWE, http://cwe.mitre.org/data/definitions/311.html, CWE-311: Missing Encryption of Sensitive Data, Web site last visited March 20, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IMPROPER AUTHORIZATION[e]

WinCC provides too many rights to several users in the database. Users with low privileges could read password fields allowing an attacker to gain access to sensitive information.

CVE-2013-0676[f] has been assigned to this vulnerability. A CVSS v2 base score of 4.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:N/A:N).[g]

RELATIVE PATH TRAVERSAL[h]

The WinCC Web server could 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. This could allow the attacker to browse the file system via URL manipulation and extract sensitive information.

CVE-2013-0679[i] has been assigned to this vulnerability. A CVSS v2 base score of 4.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:N/A:N).[j]

BUFFER OVERFLOW[k]

The WinCC Web server requires users to install ActiveX component RegReader to use certain WinCC functions. RegReader does not properly check the length of parameters; a malicious site

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0678 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:P/I:P/A:P), Web site last visited March 20, 2013.
e. CWE, http://cwe.mitre.org/data/definitions/285.html, CWE-285: Improper Authorization, Web site last visited March 20, 2013.
f. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0676 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
g. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:P/I:N/A:N), Web site last visited March 20, 2013.
h. CWE, http://cwe.mitre.org/data/definitions/23.html, CWE-23: Relative Path Traversal, Web site last visited March 20, 2013.
i. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0679 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
j. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:P/I:N/A:N), Web site last visited March 20, 2013.
k. CWE, http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, Web site last visited March 20, 2013.

can trigger a buffer overflow with possible remote code execution in the context of the user's browser. This could allow the attacker to cause a crash or to execute arbitrary code.

CVE-2013-0674[l] has been assigned to this vulnerability. A CVSS v2 base score of 6.8 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:P).[m]

IMPROPER AUTHORIZATION[n]

The WinCC Web server can allow a legitimate user to parse project files insecurely. If a legitimate user opens a manipulated project, sensitive data can be transmitted via the network or a DoS condition can occur.

CVE-2013-0677[o] has been assigned to this vulnerability. A CVSS v2 base score of 5.8 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:N/A:P).[p]

BUFFER OVERFLOW[k]

The WinCC central communications component (CCEServer) is vulnerable to a remote buffer overflow that can be triggered over the network. By sending a specially crafted packet to a dynamically assigned port, an attacker can generate a DoS condition against WinCC.

CVE-2013-0675[q] has been assigned to this vulnerability. A CVSS v2 base score of 6.1 has been assigned; the CVSS vector string is (AV:A/AC:L/Au:N/C:N/I:N/A:C).[r]

l. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0674 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

m. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:P), Web site last visited March 20, 2013.

n. CWE, http://cwe.mitre.org/data/definitions/285.html, CWE-285: Improper Authorization, Web site last visited March 20, 2013.

o. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0677 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

p. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:P), Web site last visited March 20, 2013.

q. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0675, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

r. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:A/AC:L/Au:N/C:N/I:N/A:C), Web site last visited March 20, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low to medium skill would be able to exploit these vulnerabilities.

MITIGATION

Siemens has produced a software update[s] that resolves these vulnerabilities. The update can be applied to all versions of SIMATIC WinCC starting with Version 7.1. Siemens recommends that asset owners and operators contact Siemens customer support[t] to acquire the update.

The update, WinCC Version 7.2, is also part of SIMATIC PCS7 V8.0 SP 1.[s]

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.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth

s. SSA-714398, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-714398.pdf, Web site last visited March 20, 2013.

t. Siemens Customer Support, msp.support.de@siemens.com, Web site last visited March 20, 2013.

Strategies.[u] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies,[v] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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.

ICS-CERT CONTACT

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.

u. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last visited March 20, 2013.

v. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last visited March 20, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

I see that this document is labeled as TLP = WHITE. May I distribute this to other people?
According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[w,x] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.

TLP = WHITE: Unlimited.

w. Traffic Light Protocol—International CIIP Directory, Issue 21, September 2009.
x. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed March 20, 2013.