ICS-CERT ADVISORY

ICSA-12-158-01—SIEMENS WINCC MULTIPLE VULNERABILITIES

June 6, 2012

OVERVIEW

Independent researchers Gleb Gritsai, Alexander Zaitsev, Sergey Scherbel, Yuri Goltsev, Dmitry Serebryannikov, Sergey Bobrov, Denis Baranov, Andrey Medov from Positive Technologies have identified multiple vulnerabilities in the Siemens WinCC application. In evaluating these reported vulnerabilities, Siemens identified an additional vulnerability that is included in this advisory. Siemens has produced an update that resolves all vulnerabilities except the buffer overflow in DiagAgent. DiagAgent is no longer supported, and this vulnerability can be mitigated by disabling the service. ICS-CERT has not tested this update. These vulnerabilities may be remotely exploited.

AFFECTED PRODUCTS

Siemens WinCC 7.0 SP3 web server and web applications are affected.

IMPACT

These vulnerabilities may allow an attacker to gain unauthorized access, read from, or write to files and settings on the target 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

VULNERABILITY OVERVIEW

CROSS-SITE SCRIPTING[a]

WinCC web applications are susceptible to reflected cross-site scripting because they do not filter out characters when parsing URL parameters. Exploitation of this vulnerability may give an attacker authenticated access to WinCC web applications.

CVE-2012-2595[b] has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P/A:N).[c]

XML (XPATH) INJECTION[d]

Web applications do not filter out special characters when parsing URL parameters. An attacker may exploit this vulnerability to read or write settings on the system.

CVE-2012-2596[e] has been assigned to this vulnerability. A CVSS v2 base score of 5.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:P/A:N).[f]

DIRECTORY TRAVERSAL[g]

Web applications do not sanitize URL parameters. An authenticated attacker can read arbitrary files on the system.

CVE-2012-2597[h] has been assigned to this vulnerability. A CVSS V2 base score of 6.8 has also been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:C/I:N/A:N).[i]

---

a. CWE, http://cwe.mitre.org/data/definitions/79.html, Web site last accessed June 06, 2012.
b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2595, NIST uses this ICS-CERT Advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:P/A:N), Web site last visited June 06, 2012.
d. CWE-91: XML Injection, http://cwe.mitre.org/data/definitions/91.html, Web site last accessed June 06, 2012.
e. Vulnerability Summary for CVE-2012-2596, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2596, Web site last accessed Month Day, 2012, NIST uses this ICS-CERT Advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:P/I:P/A:N), Web site last visited June 06, 2012.
g. CWE-22: Improper Limitation of a Pathname to a Restricted Directory, http://cwe.mitre.org/data/definitions/22.html, Web site last accessed June 06, 2012.

BUFFER OVERFLOW

The DiagAgent Web server is used for remote diagnostic purposes and is disabled by default. If the service is enabled, it does not sanitize user input correctly. Specially crafted input can crash the DiagAgent, disabling the remote diagnostic service.

CVE-2012-2598[j] has been assigned to this vulnerability. A CVSS V2 base score of 4.3 has also been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N).[k]

CROSS SITE SCRIPTING[l]

A Web application accepts a parameter in a HTTP GET request and interprets it as a URL. The victim's browser is then redirected to that URL.

If a victim clicks on a link that was prepared by an attacker, the victim's browser could be redirected to a malicious Web site instead of the WinCC system.

CVE-2012-3003[m] has been assigned to this vulnerability. A CVSS V2 base score of 3.4 has also been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P).[n]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities can be remotely exploited.

h. Vulnerability Summary for CVE-2012-2597, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2597, NIST uses this ICS-CERT Advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

i. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:C/I:N/A:N), Web site last visited June 06, 2012.

j. Vulnerability Summary for CVE-2012-2598, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2598, NIST uses this ICS-CERT Advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

k. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:N) , Web site last visited June 06, 2012.

l. CWE, http://cwe.mitre.org/data/definitions/79.html, Web site last accessed June 06, 2012.

m. Vulnerability Summary for CVE-2012-3003, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3003, Web site last accessed May 25, 2012, NIST uses this ICS-CERT Advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

n. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:P), Web site last visited June 06, 2012.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

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

MITIGATION

Siemens has released a security advisory that can be found here:

http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-223158.pdf

Siemens has produced an update that resolves all vulnerabilities except the buffer overflow in DiagAgent. The buffer overflow was not fixed, because the vulnerable DiagAgent is turned off by default and is no longer distributed or supported. The update is available in Update 2 for WinCC V7.0 SP3.[o] Siemens recommends applying this patch as soon as possible.

Siemens recommends not using DiagAgent, because it is no longer supported. Users can migrate to the SIMATIC Diagnostics Tool[p] or the SIMATIC Analyser.[q]

The Buffer Overflow vulnerability can only be exploited if the user starts the DiagAgent Web server manually. Siemens recommends that users check to ensure that the DiagAgent Web server is disabled and cautions users to only enable this option if and when it is needed.

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

o. http://support.automation.siemens.com/WW/view/en/60984587, Web site last accessed June 06, 2012.
p. SIMATIC Diagnostics Tool, http://support.automation.siemens.com/WW/view/en/44029135, Web site last accessed June 06, 2012.
q. SIMATIC Analyser, http://support.automation.siemens.com/WW/view/en/38645769, Web site last accessed June 06, 2012.

available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[r] 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.

ICS-CERT CONTACT

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

Email: 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.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public Web sites. All comments or questions related to this document should be directed to ICS-CERT at ics-cert@dhs.gov.

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.

r. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 06, 2012.