ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-205-01—SIEMENS SIMATIC WINCC INSECURE SQL SERVER AUTHENTICATION

July 23, 2012

OVERVIEW

Siemens has released a software update for an insecure SQL server authentication vulnerability in Siemens' SIMATIC WinCC and SIMATIC PCS 7 software. Previous versions of SIMATIC WinCC use default SQL server credentials that allowed administrative access to the database. The default credentials cannot be changed or disabled. This vulnerability can be remotely exploited, as was the case with Stuxnet malware which was known to target this vulnerability. Siemens has produced an updated version that resolves the reported vulnerability.

Note: This advisory, together with advisory "ICSA-12-205-02—Siemens SIMATIC STEP 7 DLL Vulnerability,"[a] addresses vulnerabilities first discovered in 2010 in conjunction with the discovery of Stuxnet. This vulnerability was fixed in 2010 by Siemens through a security update.

AFFECTED PRODUCTS

The following SIMATIC WinCC versions are affected:

- SIMATIC WinCC versions older than V7.0 SP2 Update 1 (V 7.0.2.1), and
- SIMATIC PCS 7 versions older than V7.1 SP2.

IMPACT

This vulnerability allows an attacker to gain unauthorized access by using the default credentials to 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 this vulnerability based on their operational environment, architecture, and product implementation.

[a] ICSA-12-205-02, http://www.us-cert.gov/control_systems/pdf/ICSA-12-205-02.pdf, Web site last accessed July 23, 2012.

BACKGROUND

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

USE OF DEFAULT CREDENTIALS[b]

The SIMATIC WinCC server uses default credentials for its SQL server database. An attacker can use these credentials to gain administrative access to the database server, allowing data reads and writes. The SIMATIC WinCC default credentials cannot be changed or disabled by users.

CVE-2010-2772[c] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[d]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be remotely exploited.

EXISTENCE OF EXPLOIT

Malware and public exploits are known to target this vulnerability.

DIFFICULTY

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

[b] CWE-798: Use of Hard-Coded Credentials, http://cwe.mitre.org/data/definitions/798.html, Web site last accessed July 23, 2012.

[c] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2772 , Web site last accessed July 23, 2012.

[d] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?adv&name=&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)&version=2, Web site last visited July 23, 2012.

MITIGATION

Siemens has addressed this vulnerability in SIMATIC WinCC V7.0 SP2 Update 1 (V 7.0.2.1) and newer. The latest software update, V7.0 SP3 Update 2, is provided at the Siemens product update page.[e] Siemens recommends that SIMATIC PCS 7 users should apply this update. The updated version removes the default credentials and switches authentication mechanisms to Windows protocols. Siemens strongly encourages installing the software updates as soon as possible. For further information please review Siemens Security Advisory (SSA-027884), which can be found at the Siemens ProductCERT Web site.[f]

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.[g] 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:

[e] Siemens SIMATIC WinCC Product Update, http://support.automation.siemens.com/WW/view/en/60984587, Web site last accessed July 23, 2012.

[f] Siemens ProductCERT Advisories, http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Web site last accessed July 23, 2012.

[g] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 23, 2012.

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP 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.