ICS-CERT ADVISORY

ICSA-12-205-02—SIEMENS SIMATIC STEP 7 DLL VULNERABILITY

July 23, 2012

OVERVIEW

Siemens has released a software update for a DLL hijacking vulnerability in SIMATIC STEP 7 and SIMATIC PCS 7 software. Previous versions of SIMATIC STEP 7 and PCS 7 allowed the loading of malicious DLL files into the STEP 7 project folder that can be used to attack the system on which STEP 7 is installed. This vulnerability can be remotely exploited, as was the case with Stuxnet malware which was known to target this vulnerability. Siemens has produced a patch that resolves this vulnerability.

Note: This advisory, together with advisory "ICSA-12-205-01—Siemens WinCC Insecure SQL Authentication,"[a] addresses vulnerabilities first discovered in 2010 in conjunction with the discovery of Stuxnet. This vulnerability was fixed in 2011 by Siemens through a security update.

AFFECTED PRODUCTS

The following Siemens products and versions are affected.

- SIMATIC STEP 7 versions prior to V5.5 Service Pack 1 (V5.5.1 equivalent), and
- SIMATIC PCS 7 versions before and including V7.1 SP3.

IMPACT

An attacker can execute arbitrary code by exploiting this vulnerability.

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-12-205-01, http://www.us-cert.gov/control_systems/pdf/ICSA-12-205-01.pdf, Web site last accessed July 23, 2012.

BACKGROUND

Siemens SIMATIC STEP 7 and PCS 7 software is used to configure and manage Siemens SIMATIC S7 PLCs. Siemens SIMATIC S7 PLCs are used in a variety of industrial applications worldwide, including energy, water and wastewater, oil and gas, chemical, building automation, and manufacturing.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DLL LOADING MECHANISM VULNERABILTY[b]

SIMATIC STEP 7 supports the loading of DLL files in STEP 7 project folders, which can be used within an attack against systems where STEP 7 is installed. An attacker can place arbitrary library files into STEP 7 project folders that will be loaded on STEP 7 startup without validation. The code will be executed with the permissions of the STEP 7 application.

CVE-2012-3015[c] has been assigned to this vulnerability. A CVSS v2 base score of 6.9 has been assigned; the CVSS vector string is (AV:L/AC:M/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 medium skill level would be able to exploit these vulnerabilities.

b. CWE-114: Process Control, http://cwe.mitre.org/data/definitions/427.html, Web site last accessed July 23, 2012.
c. NVD, http://web nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3015, 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:L/AC:M/Au:N/C:C/I:C/A:C), Web site last visited July 23, 2012.

MITIGATION

Siemens has provided the STEP 7 software update V5.5 SP1 (equivalent to V5.5.1) that resolves the vulnerability, but recommends that the latest Service Pack, V5.5 SP2, [e] be installed as soon as possible. SIMATIC PCS 7 users should also apply this update.

The updates implement a mechanism that rejects DLLs in the STEP 7 project folders, which contain executable code, thus preventing unintended execution of unchecked code. For further information please review the Siemens Security Advisory (SSA-110665) that 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.

e. Service Pack 2 for STEP 7 V5.5 and STEP 7 Professional 2010, http://support.automation.siemens.com/WW/view/en/57026339, Web site last accessed July 23, 2012.

f. Siemens ProductCERT Advisories, http://www.siemens.com/cert/advisories/, 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.

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

ICS-CERT continuously strives to improve its products and services. You can help by answering a very 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.