ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-343-01—SIEMENS FACTORYLINK MULTIPLE ACTIVEX VULNERABILITIES

January 04, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-343-01P on the US-CERT secure portal on December 09, 2011. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of Taiwan's Information and Communication Security Technology Center (ICST) has identified two vulnerabilities affecting ActiveX components in the Siemens Tecnomatix FactoryLink application. The report included buffer overflow and data corruption vulnerabilities.[a]

ICS-CERT has coordinated with Siemens; Siemens has released a patch that addresses the identified vulnerabilities. ICS-CERT has confirmed that the Siemens patch resolves the reported vulnerabilities.

AFFECTED PRODUCTS

The following Siemens Tecnomatix FactoryLink versions are affected:

- V8.0.2.54
- V7.5.217 (V7.5 SP2)
- V6.6.1 (V6.6 SP1).

IMPACT

Successful exploitation of the reported vulnerabilities could allow an attacker to perform malicious activities including denial of service and arbitrary 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 this vulnerability based on their operational environment, architecture, and product implementation.

[a] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4055; http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4056, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

BACKGROUND

Siemens Tecnomatix FactoryLink software is used for monitoring and controlling industrial processes. FactoryLink is used to build applications such as human-machine interface systems.

FactoryLink is implemented across a variety of industrial processes including oil and gas, chemicals, food and beverage, and building automation.

Siemens has announced that FactoryLink is now considered a mature product and will not offer FactoryLink after December 2012.[b]

VULNERABILITY CHARACTERIZATION

BUFFER OVERFLOW VULNERABILITY OVERVIEW

This vulnerability is exploited by inputting a long string to a specific parameter causing a buffer overflow that could allow the execution of arbitrary code.

CVE-2011-4055[c] has been assigned to this vulnerability. Siemens' assessment of the vulnerability using the CVSS[d] Version 2.0 calculator rates an Overall CVSS Score of 7.7.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable. Social engineering is required to convince the user to go to a manipulated website. This decreases the likelihood of a successful exploit.

EXISTENCE OF EXPLOIT

No publicly known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with moderate skill level could exploit this vulnerability. Social engineering is required to convince the user to go to a manipulated website. This decreases the likelihood of a successful exploit.

[b] Important Information for Siemens FactoryLink Customers. (July 2007) Retrieved November 21, 2011, from FactoryLink Supervisory Control and Data Acquisition: Siemens PLM Software: http://www.plm.automation.siemens.com/en_us/products/tecnomatix/production_management/factorylink/index.shtml, website last accessed January 04, 2012.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4055, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[d] http://nvd.nist.gov/cvss.cfm, website last accessed January 04, 2012.

DATA CORRUPTION VULNERABILITY OVERVIEW

This vulnerability is exploited by inputting arbitrary data, causing a file save to any specified location on the target system.

CVE-2011-4056[e] has been assigned to this vulnerability. Siemens' assessment of the vulnerability using the CVSS[f] Version 2.0 calculator rates an Overall CVSS Score of 7.7.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable. Social engineering may be required to execute a remote exploit via a manipulated file or web page.

EXISTENCE OF EXPLOIT

No publicly known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with moderate skill level could exploit the vulnerabilities.

MITIGATION

Siemens has released a patch to its customers to address these vulnerabilities. Customers of vulnerable versions of Siemens Tecnomatix FactoryLink should deploy the Siemens patch available at: http://www.usdata.com/sea/factorylink/en/p_nav5.asp

For more information, please see Siemens' Security Advisory announcement available at: http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/Siemens_Security_Advisory_SSA-850510.pdf.

In addition to the patch released by Siemens, Microsoft has released a kill bit to address the ActiveX vulnerabilities. Customers of vulnerable versions of Siemens Tecnomatix FactoryLink should install the Microsoft update referenced in the Microsoft Security Advisory 2562937: http://technet.microsoft.com/en-us/security/advisory/2562937.

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

[e] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4056, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[f] http://nvd.nist.gov/cvss.cfm, website last accessed January 04, 2012.

- 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 system 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.

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*[h] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[i] for more information on social engineering attacks.

ICS-CERT CONTACT

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

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

[g] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 04, 2012.

[h] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed January 04, 2012.

[i] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed January 04, 2012.

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.