# ICS-CERT ADVISORY

## ICSA-11-091-01—MULTIPLE VULNERABILITIES IN SIEMENS TECNOMATIX FACTORYLINK

April 01, 2011

## OVERVIEW

This ICS-CERT Advisory is a follow-up to ICS-CERT Alert 11-080-01.[a]

An independent researcher has identified six vulnerabilities in the Siemens Tecnomatix FactoryLink supervisory control and data acquisition (SCADA) product. The researcher has also publicly released exploit code. The researcher identified the following vulnerabilities types:

- Buffer overflow (2 vul)
- Absolute Path Traversal (3 vul)
- NULL Pointer Dereference (1 vul).

Siemens has released a patch addressing the identified vulnerablities. ICS-CERT has not yet validated this patch.

## AFFECTED PRODUCTS

These vulnerabilities affect all versions of Siemens Tecnomatix FactoryLink prior to and including Version 8.0.1.1473.

## IMPACT

Successful exploitation of the reported vulnerabilities could allow an attacker to perform multiple malicious activities including denial of service, directory traversal, and arbitrary code execution. The Vulnerability Classification section details the impacts for each of these vulnerabilities.

Impact to individual organizations depends on many factors unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on the environment, architecture, and operational product implementation.

## BACKGROUND

a. Alert, “ICS-ALERT-11-080-01—Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink,” US-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-080-01.pdf , last accessed April 01, 2011.

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

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

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

## VULNERABILITY CHARACTERIZATION

### BUFFER OVERFLOW VULNERABILITY OVERVIEW

Siemens Tecnomatix FactoryLink has two stack-based buffer overflow vulnerabilities.

The first vulnerability occurs in the CSService (7580/TCP). When the logging function of this service receives more than 1,024 bytes via the "vsprintf" function, the buffer size is exceeded. This vulnerability is remotely exploitable and results in denial of service.

The second vulnerability occurs in the vrn.exe server (7579/TCP). The vulnerability occurs when a parsing function used by vrn.exe is supplied a specially crafted input. This vulnerability is remotely exploitable and results in denial of service.

### BUFFER OVERFLOW VULNERABILITY DETAILS

#### EXPLOITABILITY

These exploits are remotely exploitable.

#### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

#### DIFFICULTY

An attacker with moderate skill level could exploit this vulnerability.

b. Important Information for Siemens FactoryLink Customers. (July 2007). Retrieved March 28, 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

## ABSOLUTE PATH TRAVERSAL VULNERABILITY OVERVIEW

Siemens Tecnomatix FactoryLink is vulnerable to absolute path traversal vulnerabilities. Exploitation of these vulnerabilities allows an attacker to traverse the file system and access files or directories that are outside of the restricted directory.

These vulnerabilities occur in the CSService service (7580/TCP) and the vrn.exe server (7579/TCP). An attacker can supply an absolute path to traverse directories and download files.

## ABSOLUTE PATH TRAVERSAL VULNERABILITY DETAILS

### EXPLOITABILITY

These exploits are remotely exploitable.

### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

### DIFFICULTY

An attacker with moderate skill level could exploit this vulnerability.

## NULL POINTER DEREFERENCE VULNERABILITY OVERVIEW

Siemens Tecnomatix FactoryLink is vulnerable to one null pointer dereference vulnerability in three windows services: CSService 7580/TCP, connsrv, and datasrv. Successful exploitation of this vulnerability could result in a denial of service.

## NULL POINTER DEREFERENCE VULNERABILITY DETAILS

### EXPLOITABILITY

An attacker must have access to the network to exploit this vulnerability.

### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

### DIFFICULTY

An attacker with moderate skill level could exploit this vulnerability.

## MITIGATION

ICS-CERT recommends that users of Siemens Tecnomatix FactoryLink software take the following mitigation steps:

- Upgrade to the latest version and install the latest patch.

  Siemens has released a patch to their 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.

  Refer to Siemens advisory regarding these vulnerabilities at: https://support.automation.siemens.com/dnl/DM/DMyNDQ4NQAA_43876783_Akt/Siemens_Security_Advisory_SSA-630126.pdf.

  Proper configuration of the system according to the readme files included with the patches can also mitigate some of these vulnerabilities.

- Review and check adherence to the recommended security precautions recommended by Siemens.

  The recommended security precautions are available at: http://support.automation.siemens.com/WW/view/en/28580051.

Organizations should minimize network exposure for all control systems devices. Critical devices should not directly face the Internet. Relocate control system networks and remote devices behind firewalls and isolate them from the business network. If remote access is required, employ secure methods such as Virtual Private Networks (VPNs).

Organizations that observe 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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[c]

c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

## 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 Control System Security Program 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.

***Can I edit this document to include additional information?*** Recipients may not edit or modify this document in any way. Please direct all comments or questions related to this document to the ICS-CERT at ics-cert@dhs.gov.