



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-080-01—MULTIPLE VULNERABILITIES IN SIEMENS TECNOMATIX FACTORYLINK

March 21, 2011

ALERT

SUMMARY

An independent researcher has published six vulnerabilities with proof of concept (POC) code in the Siemens Tecnomatix FactoryLink Supervisory Control and Data Acquisition (SCADA) product. All versions prior to and including Version 8.0.1.1473 are reported to be vulnerable to the following issues:

- Buffer overflows (remotely exploitable)
- Directory traversal (remotely exploitable)
- Denial of service.

ICS-CERT is currently coordinating with the vendor and security researcher to identify additional mitigations. ICS-CERT will provide additional information as it becomes available.

MITIGATION

ICS-CERT recommends that users minimize network exposure for all control system devices. Control system devices should not directly face the Internet.¹ Locate control system networks and 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*.²

1. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 2011.

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



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

BACKGROUND

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

FactoryLink can be implemented across a variety of processes including oil and gas, chemicals, food and beverage, building automation, and others.

ICS-CERT CONTACT

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

ICS-CERT Operations Center

1-877-776-7585

www.ics-cert.org

ICS-CERT@DHS.GOV

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.