ICS-CERT ADVISORY

ICSA-12-102-04—SIEMENS SCALANCE X BUFFER OVERFLOW VULNERABILITY

April 11, 2012

OVERVIEW

ICS-CERT has received a report from Siemens regarding a buffer overflow vulnerability in the web interface of the Scalance X Industrial Ethernet switch. This vulnerability was reported to Siemens by Jürgen Bilberger from Daimler TSS GmbH.

This vulnerability leaves the affected devices susceptible to a remote denial of service attack. Siemens has published a firmware update that addresses this vulnerability.

AFFECTED PRODUCTS

The following Scalance X products affected by this vulnerability:

- Scalance X414-3E
- Scalance X308-2M
- Scalance X-300EEC
- Scalance XR-300
- Scalance X-300

IMPACT

Successful exploitation of the reported vulnerability allows an attacker to perform malicious actions which may lead to a denial of service condition or possible arbitrary code execution. These actions may ultimately impact the process environment in which the system is deployed.

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.

BACKGROUND

Scalance X Industrial Ethernet switches are industrial grade Ethernet switches used to connect industrial components. This product line provides a web interface to manage controller configuration.

Scalance X is used in the Agriculture and Food, Critical Manufacturing, Government Facilities, Dams, Transportation Systems, Water, Chemical, Defense Industrial Base, Energy, and Communications sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW[a]

The embedded web server does not properly sanitize URLs in HTTP requests. If an attacker requests a malformed URL from the web server, a vulnerable Scalance X switch reboots, inhibits further data transmission to the switch, and may allow arbitrary code execution.

CVE-2012-1802[b] has been assigned to this vulnerability. Siemens has assigned a CVSS V2 base score of 7.8.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

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

MITIGATION

Siemens has produced firmware updates that resolve this vulnerability for the listed hardware platforms. Siemens strongly recommends installing the updates as soon as possible. Download the appropriate update from the following links:

- Firmware Update Location (Scalance X414-3E): http://support.automation.siemens.com/WW/view/en/59613294
- Firmware Update Location (Scalance X308-2M, X-300EEC, XR-300, X-300): http://support.automation.siemens.com/WW/view/en/59868786

a. http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, website last accessed April 11, 2012.

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1802, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- An overview over the Operational Guidelines for Industrial Security (with the cell protection concept): http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
- Information about industrial security by Siemens: http://www.siemens.com/industrialsecurity
- Recommended security practices by US-CERT: http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
- For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens Product CERT: http://www.siemens.com/cert

The Siemens Security Advisory is available at:

http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-130874.pdf.

In addition to applying the update provided by Siemens, 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.*[c] 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-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 11, 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.