ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-102-05—SIEMENS SCALANCE S SECURITY MODULES MULTIPLE VULNERABILITIES

April 11, 2012

OVERVIEW

ICS-CERT has received a report from Siemens regarding two security vulnerabilities in the Scalance S Security Module firewall. This vulnerability was reported to Siemens by Adam Hahn and Manimaran Govindarasu for coordinated disclosure.

The first issue is a brute-force credential guessing vulnerability in the web configuration interface of the firewall. The second issue is a stack-based buffer overflow vulnerability in the Profinet DCP protocol stack.

Siemens has published a patch that resolves both of the identified vulnerabilities.

AFFECTED PRODUCTS

The following Scalance S Security Modules are affected:

- Scalance S602 V2
- Scalance S612 V2
- Scalance S613 V2

IMPACT

Successful exploitation of the brute-force vulnerability may allow an attacker to perform an arbitrary number of authentication attempts using different password and eventually gain access to the targeted account.

Successful exploitation of the stack-based buffer overflow against the Profinet DCP protocol may lead to a denial of service (DoS) condition or possible 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 these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

The Scalance S product is a security module that includes a Stateful Inspection Firewall for industrial automation network applications. This security module is intended to protect automation devices and industrial networks against unauthorized access and to secure Ethernet-based industrial communication. This Siemens product is intended to protect trusted industrial networks from outside facing or untrusted networks. All Scalance S Security Modules provide filtering of incoming and outgoing network connections with stateful packet inspection.

This product is used predominately in Europe and Asia with a small US footprint. The primary sectors deploying Scalance S are Automotive, Defense Industrial Base, Energy, Critical Manufacturing, Transportation Systems, Chemical, and Water.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BRUTE-FORCE VULNERABILITY[a]

The web server in the Scalance S Security Module does not implement sufficient measures to prevent rapid multiple authentication attempts within a short timeframe, making it susceptible to brute-force attacks by attackers with access to the web server. If the administrative password is found, the attacker can manipulate the configuration and gain access to the trusted network.

CVE-2012-1799[b] has been assigned to this vulnerability. A CVSS V2 base score of 10.0 has also been assigned.

STACK-BASED OVERFLOW[c]

The Scalance S DCP protocol stack crashes when a specially crafted DCP frame is received, which may renders the firewall unresponsive and interrupts established VPN tunnels. Successful exploitation of this vulnerability may lead to a denial of service (DoS) condition or possible arbitrary code execution.

CVE-2012-1800[d] has been assigned to this vulnerability. Siemens has assigned a CVSS V2 base score of 6.1.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

[a] http://cwe.mitre.org/data/definitions/307.html, CWE-307: Improper Restriction of Excessive Authentication Attempts, website last accessed April 11, 2012

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1799, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[c] http://cwe.mitre.org/data/definitions/121.html , CWE-1121: Stack-based buffer Overflow, website last accessed April 11, 2012

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1800, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

EXISTENCE OF EXPLOIT

No known exploits specifically target these vulnerabilities.

DIFFICULTY

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

MITIGATION

Siemens has published a patch that resolves both of the identified vulnerabilities and strongly recommends installing the updates by using the following links:

- The Siemens Security Advisory is available at: http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-268149.pdf
- The firmware update is published on the following web site: http://support.automation.siemens.com/WW/view/en/59869684
- 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 ProductCERT: http://www.siemens.com/cert

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.*[e] 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] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 11, 2012.

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

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.