ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-186-01— PASSWORD PROTECTION VULNERABILITY IN SIEMENS SIMATIC CONTROLLERS S7-200, S7-300, S7-400, AND S7-1200

July 5, 2011

ALERT

SUMMARY

ICS-CERT is continuing to coordinate with Siemens concerning vulnerabilities affecting Siemens SIMATIC Programmable Logic Controllers (PLCs). In May of 2011, security researcher Dillon Beresford of NSS Labs[a] reported multiple vulnerabilities to ICS-CERT that affect the Siemens Simatic S7-1200 micro PLC as reported in ICS-CERT Alert 11-161-01.[b] The replay attack vulnerabilities affecting the S7-1200 also are verified to affect the SIMATIC S7-200, S7-300, and S7-400 PLCs. Siemens PLCs configured with password protection are still susceptible to a replay attack.

Commands between the affected PLCs and other devices are transmitted using the International Organization for Standardization Transport Service Access Point (ISO-TSAP) protocol. According to ICS-CERT analysis, the ISO-TSAP protocol is functioning to specifications; however, authentication is not performed nor are payloads encrypted or obfuscated. Like ISO-TSAP, many protocols used in industrial control systems were intentionally designed to be open and without security features.

ICS-CERT will publish additional information as it becomes available.

IMPACT

An attacker with access to the PLC or the automation network could intercept the PLC password and make unauthorized changes to the PLC operation.

The full impact to individual organizations is dependent on multiple factors unique to each organization. The ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and operational product implementation.

MITIGATION STRATEGIES

ICS-CERT continues to work with Siemens to develop specific mitigations for the reported vulnerabilities.

The following mitigations can be implemented to reduce the risk of impact by the reported vulnerabilities:

[a] NSS Labs, http://www.nsslabs.com, website last accessed June 10, 2011.

[b] ICS-CERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-161-01.pdf, website last accessed June 10, 2011.

- ICS-CERT and Siemens recommend that asset owners/operators apply a properly configured strong password to each PLC. Changing this password frequently and using unique passwords, when possible, will reduce exposure to this vulnerability.
- Defense-in-depth strategies for both enterprise and control system networks; see the ICS-CERT Recommended Practice document, *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*[c] and Siemens' Industrial Security website[d] for more information on how to apply these measures.
- Siemens recommends that concerned customers block all traffic to the PROFIBUS, MPI, and PROFINET protocol-based devices from outside the Manufacturing Zone by restricting or blocking Ethernet access to 102/TCP and 102/UDP, using appropriate security technology.
- Restrict remote access to enterprise and control system networks and diligently monitor any remote connections allowed; employ Virtual Private Network for any remote system connections.

Siemens has published a document regarding the vulnerability affecting the SIMATIC S7-200, S7-300, S7-400, and S7-1200 products.[e]

ICS-CERT will release information concerning additional mitigations as they become available.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

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.

Can I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public websites. Please direct all comments or questions related to this document to the ICS-CERT at ics-cert@dhs.gov.

[c] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed July 5, 2011.

[d] Siemens Industrial Security, http://www.siemens.com/industrialsecurity, website last accessed July 5, 2011.

[e] Potential Password Security Weakness in SIMATIC Controllers, http://support.automation.siemens.com/WW/view/en/51401544, website last accessed July 5, 2011.