ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-161-01—SIEMENS SIMATIC S7-1200 PLC VULNERABILITIES

June 10, 2011

ALERT

SUMMARY

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 programmable logic controller (PLC). ICS-CERT and Siemens have confirmed that these vulnerabilities could allow an attacker with automation network access to execute various unauthorized commands against the S7-1200 PLC.

On June 10, 2011, Siemens released a Security Advisory and patch to address a portion of the reported vulnerabilities.

ICS-CERT has confirmed the effectiveness of this patch and continues to work with Siemens and Mr. Beresford on the other reported problems.

ICS-CERT is releasing this Alert to inform users of the available patch for the Siemens S7-1200 PLCs.

IMPACT

Successful exploitation of these vulnerabilities could result in the loss of process control, possibly precipitating damage to critical industrial control systems (ICSs).

MITIGATION STRATEGIES

Where possible, ICS-CERT recommends that users of S7-1200 PLCs apply the patch developed by Siemens to help protect against exploitation of these vulnerabilities.

Siemens' Security Advisory and patch are available at the following locations.

Advisory:http://support.automation.siemens.com/WW/llisapi.dll/csfetch/50428932/Siemens_Security_Advisory_SSA-625789.pdf

Patch: http://support.automation.siemens.com/WW/view/en/41886031/133100

For general information on the behavior of the Simatic S7-1200 in industrial networks, go to the following location: http://support.automation.siemens.com/WW/view/en/50428932

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.

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

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

In addition to the patch, the following mitigations are recommended to reduce the risk of impact by the reported vulnerabilities.

- ICS-CERT and Siemens recommend that customers disable the embedded web server in TIA Portal Version 11 if it is not critical to operations.
- ICS-CERT and Siemens recommend that customers apply a properly configured, strong password. The same password should not be reused across the automation network, where possible.
- Apply 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*.[b]
- Restrict connections between the enterprise and control system networks, where possible.
- Restrict remote access to enterprise and control system networks and diligently monitor any remote connections allowed; employ Virtual Private Network (VPN) connections for any remote system access.

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.

[b] CSSP Recommended Practices, “Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf.