ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-356-01—SIEMENS SIMATIC HMI AUTHENTICATION VULNERABILITIES

December 22, 2011

OVERVIEW

ICS-CERT is aware of a public report by independent security researchers Billy Rios and Terry McCorkle concerning authentication bypass vulnerabilities affecting Siemens SIMATIC HMI products which are supervisory control and data acquisition/human-machine interface (SCADA/HMI) products.

According to this report, systems running affected versions of this product are accessible using a default username and password. These systems also generate an insecure authentication token for browser sessions. Prior to public disclosure, the researchers notified ICS-CERT of the vulnerabilities. ICS-CERT is continuing to coordinate mitigations with the researchers and Siemens.

Siemens was previously aware of these vulnerabilities and intends to address them in Service Packs to be released in January 2012. Please see mitigation section of this document for additional information regarding the release of the Service Packs. Siemens has also updated its product documentation with instructions for configuring a strong password and removing default passwords during initial setup.

AFFECTED PRODUCTS

According to Siemens, the following software packages are vulnerable:

- SmartAccess option package for SIMATIC WinCC flexible RT 2004, 2005, 2005 SP1, 2007, 2008, 2008 SP1, and 2008 SP2
- SIMATIC WinCC Runtime Advanced V11, V11 SP1, and V11 SP2
- Multiple SIMATIC Panels (TP, OP, MP, Mobile, Comfort)

IMPACT

Successful exploitation of these vulnerabilities could allow a hacker to log into a vulnerable system as a user or administrator.

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 environment, architecture, and product implementation.

BACKGROUND

The Siemens SIMATIC HMI product family is used as an interface between operators and corresponding PLCs. SIMATIC HMI does the following tasks: process visualization, operator control of the process, display of alarms, archiving of process values and alarms and management of machine parameters. This software is used in many industries including: food and beverage, water and wastewater, oil and gas, and chemical.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSECURE AUTHENTICATION TOKEN GENERATION.

The authentication token/cookie values set when a user (administrator) logs are predictable when non-encrypted HTTP communication is used. This can allow for an attacker to bypass authentication checks and escalate privileges.

CVE-2011-4508[a] has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSSVersion 2.0[b] calculator rates an Overall CVSS Score of 6.5.

WEAK DEFAULT PASSWORDS.

There is a default administrator password, which is weak and easily bruteforced or guessed. Siemens has changed the documentation to encourage the user to change the password upon first login.

CVE-2011-4509[c] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely against installations that are not following security practices recommended by Siemens[d] and ICS-CERT.[e]

EXISTENCE OF EXPLOIT

No known exploits specifically target these vulnerabilities.

[a] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4508. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[b] http://nvd.nist.gov/cvss.cfm,

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4510. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[d] Siemens PCS7 Security concept: http://support.automation.siemens.com/WW/view/en/22229786

[e] ICS-CERT Recommended Practices: http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

DIFFICULTY

It would be very simple to exploit the default password, it would require a greater amount of work and knowledge to exploit the insecure token generation vulnerability.

MITIGATION

The authentication token generation vulnerability will be addressed by Siemens in its "SIMATIC WinCC V11.0 SP 2 Update 1," which is to be released on January 13, 2012 or "SIMATIC WinCC flexible 2008 SP3" which is to be released on January 18, 2012.

Product documentation has been updated to tell the user how to set a proper password during initial setup to remove the risk of the default password vulnerability.

Siemens has published a statement on their Industrial Security web pages that addresses these issues. http://www.siemens.com/industrialsecurity

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.

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

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[f]

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams* [g] for more information on avoiding e-mail scams

[f] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

[g] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed December 22, 2011.

3. Refer to *Avoiding Social Engineering and Phishing Attacks*[h] for more information on social engineering attacks.

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 declines attribution. 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.

[h] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed December 22, 2011.