ICS-CERT ADVISORY

ICSA-12-263-01—SIEMENS S7-1200 INSECURE STORAGE OF HTTPS CA CERTIFICATE

September 19, 2012

OVERVIEW

Siemens has reported[a] an insecure HTTPS certificate storage vulnerability in Siemens' S7-1200 v2.x. Siemens has provided guidance to mitigate this vulnerability. This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that the vulnerability affects the following products:

- SIMATIC S7-1200 V2.x

IMPACT

An attacker may obtain a private key of the S7-1200 certificate authority for HTTPS and use it to create a forged certificate that can then be used in a Man-in-the-Middle attack.

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

Products in the Siemens SIMATIC S7-1200 programmable logic controller (PLC) family have been designed for process control in industrial environments such as manufacturing, power generation and distribution, food and beverages, and chemical industries worldwide.

a. SSA-240718, http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Web site last accessed September 19, 2012

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSECURE STORAGE OF HTTPS CA CERTIFICATE[b]

The certificate authority (CA) for HTTPS connections, which is installed on Siemens SIMATIC S7-1200 PLC, stores its private key insecurely. This key is used for signing certificates. Once this key is obtained, an attacker may create a forged certificate. This can then be used to complete a Man-in-the-Middle attack on a browser that already trusts this device's CA.

The PLC also has a private key that is used to dynamically generate its own certificate. This key is different from the CA private key and is not vulnerable to this attack.

CVE-2012-3037[c] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[d]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a medium skill would be able to exploit this vulnerability.

MITIGATION

Siemens strongly recommends the user uninstall the CA signing keys from the Web browser's certificate store. The procedure for performing this task is specific to each browser. Once this is performed, warning messages will occur when attempting to connect to an S7-1200 PLC. The

b. CWE-311: Missing Encryption of Sensitive Data, http://cwe.mitre.org/data/definitions/311.html, Web site last accessed September 19, 2012

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3037, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last accessed September 19, 2012

user can manually confirm the identity of the PLC and accept its certificate via the browser. This has to be done once for each S7-1200 PLC on the network.

ICS-CERT recommends that the process of confirming the identity of each PLC be performed on a secure network to prevent the possibility of a Man-in-the-Middle attack during the key exchange process. The fingerprint on the certificate will be specific to a PLC and is based on its private key. This key is still secret, and a forged certificate would contain a fingerprint mismatch.

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.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT 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.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[f] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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, Web site last accessed September 19, 2012.

f. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 19, 2012.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.