ICS-CERT ADVISORY

ICSA-12-283-01—SIEMENS S7-1200 WEB APPLICATION CROSS-SITE SCRIPTING VULNERABILITY

October 9, 2012

OVERVIEW

This advisory provides mitigation details provided by Siemens for a vulnerability that impacts the Siemens S7-1200 Web Application Module.

Siemens has reported[a] a cross-site scripting (XSS) vulnerability in Siemens's S7-1200 Programmable Logic Controllers (PLCs). Positive Technologies[b] discovered this vulnerability and reported it directly to Siemens. Siemens has provided mitigations and a firmware update to fix this vulnerability. Exploitation of this vulnerability would allow an attacker to partially modify application data and limit the availability of the device. This vulnerability affects the electric, critical manufacturing, chemical, and food and beverage sectors.

This vulnerability can be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that the vulnerabilities affect the following versions of S7-1200 PLCs:

- V2.x,
- V3.0.0, and
- V3.0.1.

IMPACT

An attacker that successfully exploits this vulnerability can run malicious JavaScript code on the target machine. Malicious code can execute various actions such as modify browser contents delivered from the PLC, steal session data, and issue commands from the PLC's Web server.

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.

a. SSA-279823, http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Web site last accessed October 9, 2012.
b. Positive Technologies, http://ptsecurity.com/, Web site last accessed October 9, 2012.

BACKGROUND

Products in the Siemens SIMATIC S7-1200 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.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CROSS-SITE SCRIPTING[c]

The Web application does not filter user input in a way that prevents cross-site scripting. If a user is enticed into passing specially crafted, malicious input to the S7-1200 Web application via an HTTP request (e.g., by clicking on a malicious URL with embedded JavaScript), JavaScript code can be returned and may then be executed by the user's browser. Various actions could be triggered by running malicious JavaScript code, including modification of browser content delivered from the PLC; stealing data, such as session cookies; issuing commands in the guise of the user to the PLC's Web server.

CVE-2012-3040[d] has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:C).[e]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

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

c. CWE-79: Improper Neutralization of Input During Web Page Generation, http://cwe.mitre.org/data/definitions/79.html, Web site last accessed October 9, 2012.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3040 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:C), Web site last accessed October 9, 2012.

MITIGATION

Siemens has released a security advisory[f] that details this vulnerability. It recommends users obtain the new updated firmware for Versions 3.0.0 and 3.0.1 of the S7-1200 by contacting Technical Support in their region:

- Germany: +49 (0) 911 895 7222
- Americas: +1 423 262 5710
- Asia-Pacific: +86 10 6475 7575

Siemens also advises users who are unable to apply this firmware update to use the following mitigations.

- Disable JavaScript within the Web browser used to access the S7-1200 Web server.
- Utilize a modern Web browser with integrated XSS filtering mechanisms.
- Deactivate the S7-1200 Web server wherever possible.

For this version of firmware (3.0.2), Siemens has also removed the HTTP PUT functionality, because it is not used by the S7-1200 Web server.

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 US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[g] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

f. Siemens Security Advisory, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-279823.pdf, Website last accessed October 9, 2012 .

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 9, 2012.

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,[h] 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.

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 email messages.
2. Refer to Recognizing and Avoiding Email Scams[i] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[j] for more information on social engineering attacks.

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 security 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.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed October 9, 2012.

i. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed October 9, 2012.

j. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed October 9, 2012.

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.