Siemens SIMATIC S7-1200 PLCs, version 2 and higher, are capable of running an embedded web server. Web server functionality is disabled by default in the 1200 project configuration. However, if enabled, the web server is susceptible to Cross-Site Scripting (XSS). Siemens provides a firmware update which fixes this XSS vulnerability.

**AFFECTED PRODUCTS**

- Siemens SIMATIC S7-1200 V2.x, V3.0.0 and V3.0.1

**DESCRIPTION**

If a user is enticed to activate a malicious URL directed at the S7-1200 web server IP address, the Cross-Site Scripting vulnerability could be exploited. If the attack is successful, the attacker could manipulate what the browser displays when viewing the S7-1200’s web pages, steal session cookies, or redirect the user’s browser to a malicious web site. In addition, it may be possible for attackers to issue commands to the S7-1200 web server at the user’s privilege level.

Detailed information about the vulnerability is provided below.

**VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSSv2 scoring system ([http://www.first.org/cvss/](http://www.first.org/cvss/)). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Cross-Site Scripting (XSS) Vulnerability

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), then 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; or issuing commands in the guise of the user to the PLC’s web server.

<table>
<thead>
<tr>
<th>CVSS Base Score</th>
<th>8.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS Temporal Score</td>
<td>6.5</td>
</tr>
</tbody>
</table>

**Mitigating factors:**

The S7-1200 web server is disabled by default in any new PLC configuration. If the S7-1200 web server is enabled, the user must be enticed into activating a malicious URL directed at the IP address of the PLC web server. Many modern browsers have integrated XSS protection mechanisms. The S7-1200 web functionality does not require JavaScript to be enabled within the browser.
SOLUTION
Siemens provides a firmware update for versions 3.0.0 and 3.0.1 of the SIMATIC S7-1200 PLC [1], which should be applied as soon as possible in cases where the embedded web server is utilized as it fixes the XSS vulnerability. Additionally, a HTTP PUT command is supported by the web server which does not impact security. As it is unnecessary for normal use of the S7-1200 web server, it will be removed starting with version 3.0.2.

Users who are unable to apply this firmware update can utilize 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

ACKNOWLEDGEMENT
Siemens acknowledges the following for their support and efforts:

- Dmitriy Serebryannikov, Artem Chaikin, Yury Goltsev, Timur Yunusov from Positive Technologies for coordinated disclosure.

ADDITIONAL RESOURCES
1. The firmware update can be obtained by contacting your Technical Support in your region:
   - Germany:  +49 911 895 7222
   - Americas:  +1 423 262 5710
   - Asia-Pacific:  +86 10 6475 7575
2. An overview of the operational guidelines for Industrial Security (with the cell protection concept):
3. Information about Industrial Security by Siemens:
   [http://www.siemens.com/industrialsecurity](http://www.siemens.com/industrialsecurity)
4. Recommended security practices by US-CERT:
   [http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html](http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html)
5. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

HISTORY DATA
V1.0 (2012-10-08): Publication Date

DISCLAIMER