**SSA-743465: Cross-Site Scripting Vulnerability in OZW672 and OZW772**

**Publication Date** 2016-01-15  
**Last Update** 2016-01-15  
**Current Version** V1.0  
**CVSSv2 Overall Score** 3.4

**SUMMARY**  
The latest version of the OZW672 and OZW772 communication module firmware fixes a vulnerability which could allow cross-site scripting attacks under certain conditions.

**AFFECTED PRODUCTS**  
- OZW672: All versions < V6.00  
- OZW772: All versions < V6.00

**DESCRIPTION**  
OZW devices (web servers) are used for remote monitoring of building controller devices, e.g. for monitoring of heating control or of air condition. Detailed information about the vulnerability is provided below.

**VULNERABILITY CLASSIFICATION**  
The vulnerability classification has been performed by using the CVSS scoring system in version 2 (CVSSv2) (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.

Vulnerability Description (CVE-2016-1488)  
The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

- **CVSS Base Score** 4.3  
- **CVSS Temporal Score** 3.4  
- **CVSS Overall Score** 3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

**Mitigating Factors**  
Attackers can only take advantage of the vulnerability if they are able to trick users into accessing a malicious link.

**SOLUTION**  
Siemens provides firmware updates OZW672 V6.00 [1] and OZW772 V6.00 [2] which fix the vulnerability. Siemens recommends customers to upgrade to the new firmware versions.

As a general security measure Siemens strongly recommends to protect network access to OZW products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

**ACKNOWLEDGEMENTS**  
Siemens thanks the following for their support and efforts:

- Aditya Sood for coordinated disclosure of the vulnerability
• Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts

ADDITIONAL RESOURCES

[1] The firmware updates for OZW672 products can be obtained at: https://support.industry.siemens.com/cs/ww/en/view/62567396


[3] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-01-15): Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use