SSA-963338: Multiple Buffer Overflows in UPnP Interface of OZW and OZS Products

Publishing Date	2013-01-29
Last Update	2014-06-13
Current Version	V1.2
CVSS Overall Score	8.7

Summary:

Siemens OZW and OZS products use the UPnP network protocol for supporting specific localization functions. The 3rd party library libupnp [4] used for this protocol is vulnerable to multiple stack-based buffer overflows, as reported by CERT-CC [5]. These vulnerabilities allow DoS attacks and possibly remote code execution if the affected network ports are reachable by an attacker.

Siemens addresses these issues by firmware updates [1, 2].

AFFECTED PRODUCTS

- OZW772.01, OZW772.04, OZW772.16, OZW772.64, OZW772.250: Firmware Versions < V5.10
- OZW672.01, OZW672.04, OZW672.16: Firmware Versions < V5.00
- OZW775: Firmware Versions <= V3.01
- OZS164.13, OZS164.23: Firmware Versions <= V2.00

DESCRIPTION

OZW and OZS devices (Web servers) are used for remote monitoring functions of building controller devices, e.g. for monitoring of heating control or of air condition. They are mainly used in small or medium-size buildings (typically small single-domain networks).

These products use the UPnP network protocol for enhancements of the convenience of specific localization functions; these enhancements are implemented using the libupnp library [4]. This library has multiple vulnerabilities that allow specially crafted packets to cause stack-based buffer overflows [5], resulting in Denial-of-Service attacks and possibly remote code execution against the affected products.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (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

Multiple remotely exploitable stack-based buffer overflows.

CVSS Base Score	10.0
CVSS Temporal Score	8.7
CVSS Overall Score	8.7 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)
Related CVE numbers:	CVE-2012-5958, CVE-2012-5959, CVE-2012-5960, CVE-2012-5961, CVE-2012-5962, CVE-2012-5963, CVE-2012-5964, CVE-2012-5965

Mitigating factors:

The vulnerabilities can only be exploited from remote networks if the related UPnP ports are accessible from these networks.

SOLUTION

Siemens provides firmware updates OZW772 V5.10 [1] and OZW672 V5.00 [2] which fix the vulnerabilities. Siemens recommends customers to upgrade to the new firmware versions.

For OZW775 and OZS products the risk can be mitigated either by upgrading to the product successors OZW672 or OZW772, or by implementing the following steps:

- Make sure that a firewall is implemented at the border of the trusted domain which blocks UPnP communication on UDP port 1900 to and from outside. Restrict the firewall configuration to allow as few network ports as possible.
- OZW and OZS devices should switch off UPnP advertisement by selecting the following menu options:
  Settings → Communication → Ethernet → Localization functions
- Check the local network for any signs of unusual activity.
- Visit the related customer support portal web page for more information [3].

As a general security measure Siemens strongly recommends to protect network access to OZW and OZS products with appropriate mechanisms. It is advised to follow recommended security practices [6] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- CERT Coordination Center for notification and coordination efforts.
- HD Moore of Rapid7 for vulnerability reporting and coordinated disclosure.

ADDITIONAL RESOURCES

[1] The firmware update for OZW772 products can be obtained at:
http://support.automation.siemens.com/WW/view/en/62564534

[2] The firmware update for OZW672 products can be obtained at:
http://support.automation.siemens.com/WW/view/en/62567396

[3] Customer Support Portal Web page (including document “OZW Security Advisory”)
http://support.automation.siemens.com/WW/view/en/41929231/130000

[4] Libupnp library web site:
http://pupnp.sourceforge.net

[5] CERT Vulnerability Note:
http://www.kb.cert.org/vuls/id/922681

[6] Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

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

HISTORY DATA

V1.0 (2013-01-29)	Publication date
V1.1 (2013-02-05)	Added additional technical details
V1.2 (2014-06-13)	Adjusted for final fix

DISCLAIMER