SSA-986695: Information Disclosure Vulnerability in the OZW Web Server

Publication Date:	2020-02-11
Last Update:	2020-02-11
Current Version:	V1.0
CVSS v3.1 Base Score:	5.3

SUMMARY

OZW672 and OZW772 Web Server versions < 10.00 contain a vulnerability that could allow unauthenticated users to access project files under certain conditions.

Siemens has released Version 10.00 that fixes the vulnerability and recommends to update all web servers.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
OZW672: All versions < V10.00	Update to OZW672 V10.00 https://support.industry.siemens.com/cs/document/62567396
OZW772: All versions < V10.00	Update to OZW772 V10.00 https://support.industry.siemens.com/cs/document/62564534

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Configure the product according to the OZW hardening guidelines.
- Restrict access to the device to the internal or VPN network. Further, if possible, restrict access to the OZW Web Server to trusted IP addresses.

GENERAL SECURITY RECOMMENDATIONS

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

PRODUCT 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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2019-13941

Vulnerable versions of OZW Web Server use predictable path names for project files that legitimately authenticated users have created by using the application's export function. By accessing a specific uniform resource locator on the web server, a remote attacker could be able to download a project file without prior authentication.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected system. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-552: Files or Directories Accessible to External Parties

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Maxim Rupp for reporting the vulnerability

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2020-02-11): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.