Improper Authentication, Permission, Privileges and Access Controls in VSN300 Wi-Fi Logger Card (standard and for React)

ABBVU-EPPE-ICS-VU-196220

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

Wi-Fi Card with firmware 1.8.15 and earlier releases
Wi-Fi Card for React with firmware 2.1.3 and earlier releases

Vulnerability ID

ABB ID:	ABBVU-EPPE-ICS-VU-196220
ICS-CERT ID:	ICSA-17-192-03

Summary

An update is available that resolves a publicly reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could gather information related to the network where Wi-Fi is installed. Also a malicious user, authorized as a guest, is able to disclose information that application should not provide for that account level.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS). The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

Vulnerability a) Improper Authentication

CVSS v3 Base Score:	*7.5*
CVSS v3 Vector:	*(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:R)*
CVSS v3 Link:	

https://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:R

Vulnerability b) Permission, Privileges and Access Controls

CVSS v3 Base Score:	*6.5*
CVSS v3 Vector:	*(AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:R)*
CVSS v3 Link:	

https://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:R

Corrective Action or Resolution

The problem is corrected in the following product versions:

Affected product version	Version where issue is mitigated
VSN300 Wi-Fi Card Ver. 1.8.15 and earlier	VSN300 Wi-Fi Card Ver. 1.9.0
VSN300 Wi-Fi Card for React Ver. 2.1.3 and earlier	VSN300 Wi-Fi Card for React Ver. 2.2.5 or newer

ABB recommends that customers apply the update at earliest convenience

Vulnerability Details

A vulnerability exists in the WebUI backend included in the product versions listed above.

Improper Authentication

By accessing a specific uniform resource locator (URL) on the local web server a malicious user is able to access internal information about Wi-Fi status and devices without authenticating.

Example:
GET /au/logger/v1/wifi/scan HTTP/1.0
or
GET /au/logger/v1/wifi/status HTTP/1.0

Risk: This information could be used by a malicious user to gather information related to the network where the Wi-Fi is installed. To have access to the information, the malicious user must be inside the same network (SSID and Password) as the Wi-Fi. The same information could be gathered by a PC connected in the same network.

CVE-2017-7920 has been assigned to this vulnerability.

Permission, Privileges and Access Controls

Authorized as a guest, a malicious user is able to disclose information that application should not provide for this account. The information is not available via the web-interface of the application without proper access rights.

Example:
GET / v1/config HTTP/1.0

Risk: Using the command shown in the example several information could be read.

The risk is high as the malicious user could use the information to have access to the Wi-Fi Card privileged information without authentication. The prerequisite is that the malicious user must be already inside the network and have knowledge of the Wi-Fi network: SSID and password.

CVE-2017-7916 has been assigned to this vulnerability.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network.

Such practices include that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case.

Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

Workaround are described in the *Corrective Action or Resolution* chapter above.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could gain access to reserved information on the network and to some device information.

What causes the vulnerability?
The vulnerability is caused by unchecked input data in the WebUI backend engine in the Wi-Fi card and unsecure data storage.

What are the affected products?
The WebUI interface of the Wi-Fi Card

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could gain access to reserved information of the network where the Wi-Fi card is installed and to some reserved information of the Wi-Fi card itself.

How could an attacker exploit the vulnerability?
An attacker could try to exploit the vulnerability by creating and sending special message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section *Mitigating Factors* chapter above.

Could the vulnerability be exploited remotely?
Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?
The update removes the vulnerability by modifying the way that the access is managed. Additionally all information are now moved under authenticated module layer.

When this security advisory was issued, had this vulnerability been publicly disclosed?
No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received reports that indicate that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- ICS-CERT for coordinating this vulnerability

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.