CYBER SECURITY ADVISORY

ABB Software Vulnerability Report: UnoDM, Improper Authentication

ABBVU-EPSP-4107-IT-004

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.

Affected Products

UNO-DM, version 1.8.2 and all prior versions

PVS-100-TL and PVS120-TL, version 0.10.14 and all prior versions

PVS-175-TL, version 0.2.6 and all prior versions

PVS-50/60 and TRIO-TM, version 1.2.15 and all prior versions

REACT 2, version 0.2.19 and all prior versions

Vulnerability ID

ABB ID: ABBVU-EPSP-4107-IT-004

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could cause the product to have access to some product information (nameplate, current connected IP, log), in read only mode without any login procedure

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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.

CVSS v3 Base Score: 4.0 (severity rating: medium)

CVSS v3 Temporal Score: 3.8 (severity rating: low)

CVSS v3 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

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

Recommended immediate actions

ABB is aware of public reports of a vulnerability in the product versions listed above. An attacker who successfully exploited this vulnerability could have access to some product information (nameplate, current connected IP, log) in read only mode

The problem has been corrected in the following product versions:

- UNO-DM, version 1.8.3
- PVS-100-TL and PVS120-TL, version 0.10.15
- PVS-175-TL, version 0.2.7

- PVS-50/60 and TRIO-TM, version 1.2.16
- REACT 2, version 0.2.20

ABB is constantly investigating on how to reduce the number of information shared without login access to the minimum.

ABB would recommend that customers apply the update at the earliest convenience.

Vulnerability Details

A vulnerability exists in the WebServer included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node

Mitigating Factors

Recommendation is to use the product in a local network and to not give public access to it from internet by, for example, exposing it with a NAT or equivalent solution. This reduce the risk to only people logged into the local network with related security

Recommendation is to keep the product always updated to the latest available version. This will give the product the maximum available security protection.

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

ABB recommends to prefer the Wireless connectivity, where possible, instead of Wired connectivity.

The access to Wireless connectivity is protected by a passphrase only known to the owner Moreover, the channel itself is protected and cyphered so no tampering can take place during the communication between a computer/smartphone/tablet… and the device.

If Wired connectivity is mandatory, the customer have to take it in a secured local network avoiding the exposure of the network to prying eyes using security practices Only authorized personnel to the local network shall have access to the read only information.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could have access to some information (nameplate, current connected IP, log) in read only mode.

What causes the vulnerability?

The vulnerability is caused by the fact some information have to be shared by the WebServer with the PC before a login procedure takes place.

What is the Improper Authentication?

The product exposes a Web Server to permit the user management.

Before the login procedure, the web application starts sharing information with the product to acquire nameplate data. The share data are used to adapt the behavior of the Web UI to the product.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability get some information (nameplate, current connected IP, log) in read only mode.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the 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 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 capability to have access to the log if the device while it keeps the access to nameplate information

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 any information indicating 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:

Maxim Rupp for discovering this vulnerability.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

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