DOCUMENT ID: 2PAA121681
REVISION: B
DATE: 2020-05-14

CYBERSECURITY ADVISORY

SECURITY ABB Device Library Wizard Information Disclosure Vulnerability

CVE ID: CVE-2020-8482

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

ABB Device Library Wizard versions 6.0.X, 6.0.3.1, 6.0.3.2

Scope of this document

This document provides information about the security vulnerability discovered in Device Library Wizard in certain versions as mentioned under the section *Affected products*.

Vulnerability ID and Product Issue Number

CVE ID	Product Issue Number*
CVE-2020-8482	800xADLW-IN-6032-001

* Product Issue Number - is an ABB internal unique identifier to identify an issue. The Product Issue Number is for example used to identify the correction of a problem in a Release Note.

Summary

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

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.

CVE-2020-8482 - ABB Device Library Wizard - Information Disclosure

CVSS v3.0 Base Score:	7.8 (High)
CVSS v3.0 Temporal Score:	7.5 (High)
CVSS v3.0 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.0 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-8482

Recommended immediate actions

ABB recommends changing any user account passwords which is suspected to be known by an unauthorized person. Interactive logon (both local and remote) is recommended to be disabled for the system service account.

The problem is corrected in the following product versions:

- Device Library Wizard version 6.0.3.2 RU1
- Device Library Wizard version 6.0.3.3
- Device Library Wizard version 6.1.X onwards

ABB recommends that customers apply the update at the earliest convenience.

If the affected version, as described above is used and an update cannot be applied soon, please contact ABB for further assistance.

Check that the usage of the Access Enable key in AC 800M HI and the configured access level of SIL variables corresponds to the risk analysis. See the FAQ “Can functional safety be affected by an exploit of any of these vulnerabilities?” below.

Vulnerability details

A vulnerability exists in Device Library Wizard in the affected product versions listed above. It creates a file that contains confidential data that could be read by low privileged users. This could allow the attacker to take control of one or multiple system nodes.

Mitigating factors

The main mitigating factor is that an attacker needs to be able to login to an account in the system, so the primary mitigation against these attacks is to ensure that only authorized persons have access to user accounts on the system nodes. This also includes any user accounts accessing the system via remote tools like Remote Desktop. Interactive logon to service accounts should be blocked. See also section Recommended immediate actions above.

Recommended baseline security practices and firewall configurations can help protect a network and its attached devices from attacks that originate from outside the network. For example, common practices are for process control systems to be 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 must be evaluated case by case.
Process control and automation systems should not be used for general business functions (e.g. Internet browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

More information on recommended practices can be found in the section References

Workarounds

None.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could take control of one or multiple system nodes.

What causes the vulnerability?

This is caused by SW writing excessive confidential information into an unprotected file.

What is the Device Library Wizard?

The Device Library Wizard is a tool used in System 800xA for adding supported Device Types of FOUNDATION Fieldbus, HART and PROFIBUS. The Device Types are provided by ABB on a continuous basis as and when the Device Types are released by the Device Integration Center.

For more information on Device Library Wizard, refer to the Device Library Wizard user manual (2PAA102573*).

What might an attacker use the vulnerability to do?

See section Vulnerability details above.

Can functional safety be affected by an exploit of any of these vulnerabilities?

This question is relevant if AC 800M HI is used in the same System 800xA as the affected Device Library Wizard.

Under certain conditions exploits of this vulnerability may affect the integrity of safety functions in System 800xA. This is however prevented if the Access Enable key in the AC 800M HI is turned Off (“disabled”) and Access Level for the variables in the safety applications are configured to “Read Only” or “Confirm and Access Enable” (see 3BNP004865* AC 800M High Integrity Safety Manual for more information regarding SIL Access Control and Confirmed Write Support).

With other usage of the Access Enable key and the SIL variable Access Level, exploits of this vulnerability may affect the integrity of safety functions in System 800xA. This risk could be avoided by changing to the described safe configuration or by following the advice in section “Recommended immediate actions” above.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by logging into the affected node as a low privileged user, read confidential data from an unprotected file.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access and access to an account that can login to the system node remotely 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. See section Mitigating factors above.

What does the update do?

The update removes the information disclosure vulnerability and it removes superfluous confidential 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.

Acknowledgement

ABB thanks Applied Risk for helping to identify the vulnerabilities and protecting our customers.

References

3BSE080520* System 800xA, Security Deployment Guide.

3BSE041389* 800xA System, Engineering Planning and Concepts.

3BSE034463* System 800xA Network Configuration.

Support

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

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

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2020-04-30
B	all	Misc clarifications	2020-05-14