SECURITY BULLETIN - HART Vulnerability in ABB Third Party Device Type Library

Notice

Affected Products

- **ABB Third Party Device Type Library - Version 1.17 and all earlier**
  for usage with 800xA - Device Management HART
- **Freelance ABB 3rd Party HART DTMLibrary – Version 1.4.178.214 and all earlier**
  for usage with Freelance 800F
- **S Plus Melody ABB 3rd Party HART DTMLibrary – Version 1.4.175.185 and all earlier**
  for usage with Symphony Plus with Composer Melody, S+Engineering for Melody, and Composer Field.

Vulnerability ID

ABBVU-PACT- 2PAA114210

Summary

ABB is aware of public reports of a vulnerability in a SW component that ABB Third Party Device Type Library is based on. An update is available that resolves a publicly reported vulnerability in the underlying SW of the product versions listed above.

An attacker who successfully exploited this vulnerability could cause the software used for field device configuration (FDT Frame Application) in above ABB systems to stop. The software is used for configuration or monitoring purposes only. No loss of information or loss of control or view by the control system results from an attacker successfully exploiting this vulnerability.

Severity rating

The severity rating for this vulnerability is Low, with the overall CVSS score 1.8 (the CVSS vector string is AV:A/AC:H/AU:N/C:N/I:N/A:P/E:ND/RL:ND/RC:ND). This assessment is based on the types of systems that are affected by the vulnerability, how difficult it is to exploit, and the effect that a successful attack exploiting the vulnerability could have.

Corrective Action or Resolution

The problem is corrected in the following product versions:

ABB Third Party Device Type Library - Version 1.19
for usage with 800xA - Device Management HART

Freelance ABB 3rd Party HART DTMLibrary – Version 1.4.180.225
for usage with Freelance 800F

S Plus Melody ABB 3rd Party HART DTMLibrary –Version 1.4.180.225
for usage with Symphony Plus with Composer Melody, S+Engineering for Melody, and Composer Field.

ABB recommends that customers apply the update at earliest convenience

For more details on the upgrade procedure, refer to Release Notes:

- 2PAA105430R20 System 800xA ABB Third Party Device Type Library V1.19 ReleaseNotes HART
- 2PAA107705R03 Freelance ABB 3rd Party HART DTMLibrary 1.4.180.225
- 2VAA101417R05 S Plus Melody ABB 3rd Party HART DTMlibrary 1.4.180.225

Vulnerability Details

A vulnerability exists in the CodeWrights GmbH HART Device Type Manager (DTM) library included in the product versions listed above. An attacker could exploit the vulnerability by sending a malformed HART command response causing the DTM software to hang. The FDT Frame Application needs to be restarted to overcome the problem.

The field device itself and other parts of the control system are not affected.

This exploit is possible from the network between the FDT Frame application and the HART transmitter on the 4-mA to 20-mA current loop.
Note that an attacker would require physical access to the HART loop or access to a compromised network between the HART loop and the FDT-Frame Application. In the latter case the encapsuation of the HART command response on different network layers would need to be understood to inject a malformed message. This increases the difficulty to expoit the 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 (including the 4..20 mA current loop for connecting field devices) 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. 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.

Using a virus scanner on all Windows-based system nodes, with the latest updates and with on-access scanning enabled on all Windows-based system nodes, can help prevent infection by malicious or unwanted software.

More information on recommended practices can be found in the following documents:

3BSE032547, Whitepaper - Security for Industrial Automation and Control Systems

Workarounds

Not applicable.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could stop the FDT-Frame-Application and prevent further configuration or monitoring of field devices.

What causes the vulnerability?

The vulnerability is caused by an insufficient input validation for the communication data in Device Type Managers (DTM) of ABB Third Party Device Type Library running in the FDT-Frame-Application of the control system.

What is the ABB Third Party Device Type Library?

ABB Third Party Device Type Library is a library of Device Type Managers (DTMs) that ABB provides to configure and diagnose HART-field-devices from 3rd party vendors when these are connected to ABB Control Systems. DTMs are drivers for the specific devices that provide the user interface to work with the field devices and run in so-called FDT-Frame-Applications. The applicable Frame-Applications from ABB are Fieldbus Builder HART of 800xA Device Management HART, Control Builder F of Freelance 800F, and Composer Melody, S+Engineering for Melody, and Composer Field..
Note: ABB Third Party Device Type Library is not an integral part of the Control Systems' software. It is only available with the System when it has been installed explicitly, e.g. form the System's media or after download from ABB's Solutionbank.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the FDT-Frame-Application to stop on the node where a DTM out of ABB Third Party Device Type Library is running

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a malformed HART command response that is sent to the DTM. This would require that the attacker has access to the 4..20 mA current loop that the field device is connected to. Physical access to this current loop is required.

Could the vulnerability be exploited remotely?

No, the exploit requires physical access to the current loop is required or control over a system node in the communication chain between the HART loop and the FDT-Frame Application. 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 improving the input validation for the communication data in Device Type Managers (DTM) of ABB Third Party Device Type Library.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed for different versions of the underlying SW component.

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:

- Alexander Bolshev of Digital Security for identifying the vulnerability of improper input to DTMs through the the 4-mA to 20-mA current loop.

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.

1. REVISION

Revision	Page	Description	Date Dept/Init
-	all	New document	11022015/DEATG/LTPF/blm