ABB DOC ID: 2CMT2018-005723
REVISION: 02
DATE: 2018-06-15

CYBER SECURITY ADVISORY

Vulnerability in Pluto Manager – DLL Hijacking

ABBVU-EPPC-3122-Sweden-001

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

Pluto Manager versions 2.24-2.34.3

Vulnerability ID

ABB ID: ABBVU-EPPC-3122-Sweden-001

Summary

An update is available that resolves a privately reported vulnerability in the product versions listed above. An attacker who successfully exploited this vulnerability could insert and run arbitrary code.

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:	6.6 (Medium)
CVSS v3 Temporal Score:	6.1 (Medium)
CVSS v3 Vector:	AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H/E:F/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:R/S:U/C:L/I:L/A:H/E:F/RL:O/RC:C

Recommended immediate actions

The problem is corrected in the following product versions:

Pluto Manager version 2.36

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

Vulnerability Details

An uncontrolled search path element (DLL Hijacking) vulnerability has been identified in the application versions listed above. To exploit this vulnerability, an attacker could rename a malicious DLL to meet the criteria of the application, and the product would not verify the correctness of the DLL. Once DLL is loaded by the application, the DLL could run malicious code at the same privilege level as the application. Administration rights are not needed but user interaction is required to make use if this vulnerability.

Mitigating Factors

Recommended security practices can help protect computer from executing malicious software. Such practices include ensuring PC are running recent antivirus software and that virus definitions are updated automatically on regular basis, on-access scanner is enabled which runs in background and actively scans the PC for viruses and other malicious threats.

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

2TLC172002M0218, Pluto Programming Manual

Workarounds

ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. The list below contains different workarounds that are related. The first workaround is recommended as this prevents user from opening Pluto Manager when double clicking on project file. However, this workaround requires changes on the PC. If the user cannot make such changes, then the alternative is to apply the second workaround.

1. Remove Pluto Manager as default program for files with extension .sps and .fps.
2. Do not start Pluto Manager by double clicking on Pluto manager project file.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could insert and run arbitrary code on an affected PC.

What causes the vulnerability?

The vulnerability is caused by the uncontrolled search path that is used by the product when loading a certain DLL.

What is the affected product?

The affected product is Pluto Manager that is the programming tool for Pluto Safety PLC.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to insert and run arbitrary code with the same privileges as the product.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by sending a bunch of targeted project files together with a malicious DLL. This can be done by mail, file-share or thumb drive. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need either prior access to affected PC or physical access to affected PC.

What does the update do?

The update removes the vulnerability by modifying the search path to not include current working folder when loading DLL files. For the specific DLL causing the vulnerability the search path has been changed to be an absolute path.

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?

Yes, ABB had 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:

Herman Groeneveld, Independent Security Researcher, for contributing with information about the vulnerability and providing proof of concept.

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.