Security Advisory – DataManagerPro File Permissions Escalation Vulnerability

ABB-VU-BUMP-089290

Update Date:

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 DataManagerPro – Data Review Software

All versions: 1.0.0 to 1.7.0

Summary

ABB is aware of a privately reported vulnerability in the product listed above.

An attacker who successfully exploited this vulnerability could insert and run arbitrary code on a computer where the affected product is used.

An update is available that resolves the issue.

Severity rating

The severity rating for this vulnerability is High, with the overall CVSS v2 score of 6.0 and CVSS v3 score of 7.2

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.

CVSS v2 Overall Score: 6.0

CVSS v2 Vector: *AV:L/AC:H/Au:S/C:C/I:C/A:C*

CVSS v2 Link:
https://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=(AV:L/AC:H/Au:S/C:C/I:C/A:C)

CVSS v3 Overall Score: 7.2

CVSS v3 Vector: AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

CVSS v3 Link:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

Corrective Action or Resolution

The problem is corrected in the following product versions:

ABB DataManagerPro version 1.7.1

ABB recommends that customers apply the update at earliest convenience

Vulnerability Details

A vulnerability exists in the istallation script for the product versions listed above. When running the software as an Administrator, a Local user may elevate permissions to Administrator by swapping DLL's in a package when an Admin user logs in.

Mitigating Factors

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

Such practices include:

- Carefully inspecting any files transferred between computers, including scanning them with up to date antivirus software, so that only legitimate files are being transferred.
- User account management, appropriate authentificaton and permission management using the principle of least privilege.

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

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

Workarounds

ABB has not identified any workarounds.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could insert and run arbitrary code in an affected system node.

What causes the vulnerability?
The vulnerability is caused by an error in the installation script of the application

What is the product?

DataManagerPro is a tool for analysis of measurement data recorded by a ScreenMaster paperless recorder.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability may insert and run arbitrary code.

How could an attacker exploit the vulnerability?
An attacker that manages to get malicious code to a specific directory in the file system of a computer where DataManagerPro is used, could get this code executed by an authenticated and legitimate user of DataManagerPro.
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 to have physical access to an affected system node.

What does the update do?
The update removes the vulnerability by modifying the software installation script.

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. Only a proof-of-concept has been demonstrated.

Acknowledgements

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

- The Zero Day Initiative for forwarding the reported vulnerability description to ABB.

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.