SECURITY Advisory - Panel Builder 800 5.x vulnerability

ABB-VU-PACT-Panel800-CN-510-012

Update Date: <*not updated*>

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

Panel Builder 800 version 5.1 and earlier

Vulnerability ID

ABB-VU-PACT-Panel800-CN-510-012

Summary

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

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

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?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

Panel Builder 800 version 6.0 is not affected by this problem. ABB recommends any new projects to use this version and Panel 800 hardware of the associated version.

ABB recommends any customers wanting to still use Panel Builder 800 version 5.1 and Panel 800 hardware of the associated version to use the Workaround described below.

Vulnerability Details

An attacker that manages to get malicious code to a specific directory in the file system of a computer where the Panel Builder 800 version 5.1 is used, could get this code executed by an authenticated and legitimate user of the Panel Builder 800 version 5.1.

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:

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

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

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

Workarounds

ABB has tested the following workaround. It will not correct the underlying vulnerability but it will block the known attack vector:

Remove the association of .pba files with the Panel Builder.

This can be done via:
Control Panel\Programs\Default Programs\Set Associations

This workaround has the impact that it will no longer be possible to start the Panel Builder 800 version 5.1 by a double click of a Panel 800 project file. The Panel Builder 800 version 5.1 will need to be started from a link provided by the product installation, e.g. in the Windows start menu.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could get arbitrary code executed in an affected computer.

What causes the vulnerability?

The vulnerability is caused by some of the components in the Panel Builder 800 5.1 implementing improper assumptions of locations of other components.

What is the Panel Builder 800?

The Panel Builder 800 is an engineering tool for the process panels included in the product suite Panel 800.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this could 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 the Panel Builder 800 version 5.1 is used, could get this code executed by an authenticated and legitimate user of the Panel Builder 800 version 5.1. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, an attacker must get malicious code to a specific directory in the file system of a computer where the Panel Builder 800 Version 5.1 is used, then get a legitimate user of the Panel Builder 800 Version 5.1 to execute it.

What does the new version do differently?
Panel Builder 800 version 6.0 does not have this vulnerability since it has a stricter control of its components.

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:

- Ivan Sanchez from Nullcode Team for discovering this vulnerability and bringing the incident to our attention and working with us on the response.

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.

REVISION

Rev. ind.:	Page (P) Chapt. (C)	Description	Date Dept.
-		New document	2016-03-14 PACT/XA/A