
CYBER SECURITY ADVISORY

SECURITY - Panel Builder 800, Improper input validation vulnerability

ABBVU-IACT-Panel800-CN-510-013

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.

© Copyright 2018 ABB. All rights reserved.

Affected Products

Panel Builder 800 all versions

Vulnerability ID

ABB ID: ABBVU-IACT-Panel800-CN-510-013

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.

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: 7.0 (High)

CVSS v3 Temporal Score: 6.4 (Medium)

CVSS v3 Vector: AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C

CVSS v3 Link:

<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C>

Recommended immediate actions

ABB is currently investigating this vulnerability in order to provide adequate protection to customers. The problem will be corrected in future product versions. This advisory will be updated when a corrected version is available.

Until a corrected version is available customers are recommended to follow the advice under "Mitigating Factors" below.

Vulnerability Details

A vulnerability exists in the file parser in the product versions listed above.

An attacker could exploit the vulnerability by tricking a user of the product to open a specially crafted file, allowing the attacker to insert and run arbitrary code.

Please note that this vulnerability is not exploitable remotely and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the affected product and loads the specially crafted file.

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

- Conduct or reinforce cyber security awareness training for users of Panel Builder 800
 - Describing general cyber security best practice recommendations for industrial control systems.
 - Informing that it is possible to infect Panel Builder files with malware.
 - Describing the importance of being careful with files that are received unexpectedly and/or from unexpected sources.
- 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 documents:

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

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 improper input validation in the file parser in the Panel Builder 800.

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 insert and run arbitrary code.

How could an attacker exploit the vulnerability?

An attacker could create a specially crafted file and try to trick a person using the Panel Builder 800 to open this file.

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 be able to provide a specially crafted file to a legitimate user of the affected product, and to trick this person to use the file.

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.

Acknowledgements

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

Michael DePlante of Leahy Center for Digital Investigation at Champlain College and Michael Flanders of Trend Micro, both working with Trend Micro's Zero Day Initiative 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 <https://new.abb.com/contact-centers>.

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