ABB DOC ID: 3BSE091042
REVISION: A1
DATE: 2018-11-26

CYBER SECURITY ADVISORY

# SECURITY - CP400 Panel Builder TextEditor 2.0, Improper input validation vulnerability

ABBVU-IACT-3BSE091042

## Notice

# Affected Products

CP400PB, Panel Builder for CP405 and CP408, versions 2.0.7.05 and prior.

# Vulnerability ID

ABB ID: ABBVU-IACT-3BSE091042

# 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 cause the Text Editor of CP400PB to stop and potentially insert and run arbitrary code on the computer where the Text Editor 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

The problem is corrected in the following product versions:

CP400PB, Panel Builder for CP405 and CP408, versions 2.1.7.21 and later

ABB recommends that customers apply the update at earliest convenience

# Vulnerability Details

A vulnerability exists in the file parser in the TextEditor.
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 400
    - 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 Text Editor of CP400PB.

## What is the Text Editor of CP400PB?

CP400PB, the Panel Builder for CP405 and CP408, is the software application suite used for configuring the Control Panels CP405 and CP408.

The Text Editor is one of the auxiliary applications in this suite. It is an application used for preparing text strings for multi-language support for the panels during the engineering the content of the CP405 and CP408.

## What might an attacker use the vulnerability to do?

An attacker who successfully exploited this could (cause the Text Editor to stop or become inaccessible and to) 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 Text Editor to open this file.
Recommended practices help mitigate such attacks, see section Mitigating Factors above.

### Is the security of the control panels or their applications affected?

The vulnerability primarily affects the availability of the Text Editor and potentially the integrity of the computer where the Text Editor is used. It does not directly affect the security of the control panels, the equipment that they control or any other process equipment. If an attacker manages to get malicious code executed on the computer where the Text Editor is used, this could potentially be used to prepare a malicious application for the control panels.

### 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:

Ivan Sanchez from Nullcode Team for discovering this vulnerability and bringing the incident to our attention and verifying effectiveness of the fix.

## 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.