ABB PCM600 vulnerabilities

ABB-VU-PPMV-1MRS758347

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

- PCM600 up to and including version 2.6

Summary

Four vulnerabilities have been privately reported in the product versions listed above. An update is available that resolves all reported vulnerabilities.

- ABB-VU-PPMV-1MRS758347-DR1231 - Weak password hashing in ACTConfig
- ABB-VU-PPMV-1MRS758347-DR1232 - Wrong program behavior with Main Application Password
- ABB-VU-PPMV-1MRS758347-DR1233 - Insecure password storage
- ABB-VU-PPMV-1MRS758347-DR1234 - Insecure authentication data storage

Severity rating

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.

ABB-VU-PPMV-1MRS758347-DR1231 - Weak password hashing in ACTConfig

CVSS Overall Score: 2.3 (Low)

CVSS Vector: *AV:L/AC:M/Au:S/C:P/I:P/A:N/E:POC/RL:OF/RC:C*

CVSS Link:
https://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L;AC:M;Au:S;C:P;I:P;A:N;E:POC;RL:OF;RC:C)

ABB-VU-PPMV-1MRS758347-DR1232 - Wrong program behavior with Main Application Password

CVSS Overall Score: 2.5 (Low)

CVSS Vector: *AV:L/AC:L/Au:S/C:P/I:P/A:N/E:POC/RL:OF/RC:C*

CVSS Link:
https://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:L/Au:S/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

ABB-VU-PPMV-1MRS758347-DR1233 - Insecure password storage

CVSS Overall Score: 3.4 (Low)

CVSS Vector: *AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C*

CVSS Link:
https://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L;AC:L;Au:S;C:P;I:P;A:P;E:POC;RL:OF;RC:C)

ABB-VU-PPMV-1MRS758347-DR1234 - Insecure authentication data storage

CVSS Overall Score: 2.3 (Low)

CVSS Vector: *AV:L/AC:M/Au:S/C:P/I:P/A:N/E:POC/RL:OF/RC:C*

CVSS Link:
https://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L;AC:M;Au:S;C:P;I:P;A:N;E:POC;RL:OF;RC:C)

Corrective Action or Resolution

The problem is corrected in the following product versions:

PCM600 version 2.7

ABB recommends that customers apply the update at earliest convenience

Vulnerability Details

ABB-VU-PPMV-1MRS758347-DR1231 - Weak password hashing in ACTConfig

The Main Application Password in the ACTConfig configuration file is hashed with a weak hashing function. In order to exploit the vulnerability, the attacker needs to have local access to the PC running PCM600.

An attacker who successfully exploited this vulnerability can edit the “main application”.

ABB-VU-PPMV-1MRS758347-DR1232 - Wrong program behavior with Main Application Password

After changing the *Main Application Password*, it is stored insecurily. In order to exploit the vulnerability, the attacker needs to have local access to the PC running PCM600.

An attacker who successfully exploited this vulnerability can edit the *Main Application*.

ABB-VU-PPMV-1MRS758347-DR1233 - Insecure password storage

OPC Server IEC61850 authentication passwords are temporarily stored insecurely. In order to exploit the vulnerability, the attacker needs to have local access to the PC running PCM600.

An attacker who successfully exploited this vulnerability could gain access to connected devices.

ABB-VU-PPMV-1MRS758347-DR1234 - Insecure authentication data storage

PCM600 authentication credentials are stored insecurely. In order to exploit the vulnerability, the attacker needs to have local access to the PC running PCM600. The access control in PCM600 needs to be active.

An attacker who successfully exploited this vulnerability could gain access to PCM600.

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 that process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

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

1MRS758440, Protection and Control IED Manager PCM600 Cyber Security Deployment Guideline

http://search.abb.com/library/Download.aspx?DocumentID=1MRS758440&Action=Launch

Workarounds

No workarounds available.

Frequently asked questions

What is *Main Application*?

Main Application, a PCM600 term, is the graphical representation of the configuration. It can be protected with a password. The password works as a locking mechanism to prohibit accidental editing of the *Main Application*.

Using the password for locking the *Main Application* is not considered a security function in PCM600. Users may decide not to use password locking.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have access to the computer running PCM600.

What does the update do?

The update removes the vulnerability by changing the weaker hashing functionality to stronger SHA-512.

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:

- Ilya Karpov from Positive Technologies

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.