ABB DOC ID: 2CMT2020-005913
REVISION: A
DATE: 2020-04-22

CYBERSECURITY ADVISORY

Vulnerability in UPS Adapter CS141 – Path traversal

ABBVU-ELSP-4178-2150

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 2020 ABB. All rights reserved.

Affected Products

The vulnerability affects the products listed in Table 1. Affected firmware versions are 1.66 – 1.88.

Product number	Product name
4NWP102879R0001	CS141 Advanced - Box
4NWP102880R0001	CS141 Advanced - Slot
4NWP102881R0001	CS141 ModBus - Box
4NWP102882R0001	CS141 ModBus - Slot
4NWP102687R0001	CS141 Basic - Box
4NWP102688R0001	CS141 Basic - Slot

Table 1: List of affected products

Vulnerability ID

ABB ID: ABBVU-ELSP-4178-2150

CVE ID: CVE-2020-11420

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above. An update is available that resolves a privately reported vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability is allowed to read arbitrary files from the affected product including application, credentials and operating system files.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. 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 v3.1 Base Score: 6.5 (Medium)

CVSS v3.1 Temporal Score: 6.0 (Medium)

CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C

CVSS v3.1 Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C

Recommended immediate actions

The problem is corrected in the following product versions:

CS141 firmware version 1.90.

ABB recommends that customers apply the update at the earliest convenience.

Vulnerability Details

A vulnerability exists in the UPS Adapter CS141 included in the product versions listed above. An attacker with Admin or Engineer login credentials could exploit the vulnerability by manipulating variables that reference files and by doing this achieve access to files and directories outside the web root folder. An attacker may access arbitrary files and directories stored in the file system, but integrity of the files are not jeopardized as attacker have read access rights only. This attack is commonly known as *Path Traversal* or *Directory Traversal*.

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.

This vulnerability can only be exploited if attacker knows the Admin or Engineer login password. A good practice to make an attack that exploits this vulnerability more difficult is to change all default passwords as default passwords are easy to find and often used by attackers.

Workarounds

ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

- Change all default passwords to prevent attacker from login to system using default passwords.

  Impact of workaround - No functionality is reduced

- Protect the process control network from attacks that originate outside by blocking HTTP (port 80) and HTTPS (port 443) in firewall that separates process control network from another network.

  Impact of workaround - Remote monitoring service will not be available as user cannot connect to web server outside process control network.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could read arbitrary files and directories from the UPS Adapter CS141.

What causes the vulnerability?

The vulnerability is caused by unchecked input data in UPS adapter CS141.

What is the UPS Adapter CS141?

The affected product is different variants of the UPS Adapter CS141. These cards are used to monitor the UPS status (measures and states) and can also send automatic notification based on configured events (via email or SNMP traps). Having standard protocols (i.e. Modbus and SNMP) allows the user to integrate the UPS in the Building Monitoring System (BMS).

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to read arbitrary files including credential files. An important aspect is that all credential files are encrypted. This means that an attacker that successfully reads out a password file will have to decrypt the file before being able to read the password in clear text.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by manipulating variables that reference files and then possibly achieve read access to files and directories outside the web root folder. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. This would also require that the attacker is able to login as either Admin or Engineer prior to trying to exploit this vulnerability. This can be achieved if attacker know the login credentials or manages to break the authentication. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, 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.

What does the update do?

The update eliminates the vulnerability by adding an input control of the requested resources, allowing only requests of predefined files (i.e. events log) and disallowing any other request.

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:

Eduardo Cataño Conde, independent researcher, for reporting this vulnerability and providing proof of concept.

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 cybersecurity program and capabilities can be found at www.abb.com/cybersecurity.