ABB DOC ID: 9AKK108368
REVISION: A
DATE: 2021-05-06

CYBER SECURITY ADVISORY

Cassia Access Controller for ABB instance path traversal

ABBVU- ABBVREP0032- 3AXD10001382718

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

Cassia Access Controller for ABB Ability™ Smart Sensor v1.4.3

Vulnerability ID

ABB ID: ABBVU- ABBVREP0032-3AXD10001382718

ICS CERT: https://us-cert.cisa.gov/ics/advisories/icsa-21-119-02

CVE ID: CVE-2021-22685

Summary

At ABB, the security and privacy of our customers' and employees' data has our highest priority, and we continuously monitor security risks and protection. As part of an external security check, a vulnerability was found on the Cassia Access Controller for ABB Ability™ Smart Sensor.

We are pleased to report that we did not find any evidence that customers' data had been exposed. Only a very limited number of internal ABB employees email address might have potentially been unveiled.

Together with our gateway supplier, ABB has patched the affected service.

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:	6.2
CVSS v3 vector:	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v3 link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Recommended immediate actions

No actions required. Vulnerable system has been patched.

Vulnerability Details

A vulnerability existed in the Cassia Access Controller used by ABB Ability™ Smart Sensor. An attacker could have exploited the vulnerability by sending a specially crafted message to the system node, exposing file content.

Mitigating Factors

Although vulnerable system has been patched, ABB recommends continuously review and monitor the security of the gateway devices. Users should always choose strong passwords.

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.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could have got access to the file content in an affected system node. Common weakness enumeration:

- CWE-22 : Path Traversal

What is the affected product?

Affected product is Cassia gateway access controller for ABB Ability™ Smart Sensor.

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:

Claroty Research Team

Cassia Networks

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.