CCLAS input validation vulnerabilities

ABBVU-PGGA-201706

Update Date:

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

CCLAS versions prior to 6.5

Summary

ABB is aware of security vulnerabilities identified in the above versions of CCLAS that can allow an authenticated user access to files on the local file system through a Path Traversal flaw. A Cross Site Scripting vulnerability has also been discovered which can allow an unauthenticated user to execute JavaScript in victim’s browser.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and 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.

Path traversal in /ria/file

CVSS v2 Base Score:	7.8
CVSS v2 Temporal Score:	6.1
CVSS v2 Vector:	*AV:N/AC:L/Au:N/C:C/I:N/A:N/E:POC/RL:OF/RC:C*
CVSS v2 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=(AV:N/AC:L/Au:N/C:C/I:N/A:N/E:POC/RL:OF/RC:C)

CVSS v3 Base Score:	8.6
CVSS v3 Temporal Score	7.7
CVSS Vector:	*CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C*
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Path traversal in /ria/bind

CVSS v2 Base Score:	6.8
CVSS v2 Temporal Score:	6.9
CVSS v2 Vector:	AV:N/AC:L/Au:S/C:C/I:N/A:N/E:POC/RL:OF/RC:C
CVSS v2 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=(AV:N/AC:L/Au:S/C:C/I:N/A:N/E:POC/RL:OF/RC:C)

CVSS v3 Base Score:	7.7
CVSS v3 Temporal Score	6.9
CVSS Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C

Cross Site Scripting (XSS)

CVSS v2 Base Score: 6.4

CVSS v2 Temporal Score: 4.9

CVSS v2 Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C

CVSS v2 Link: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=(AV:N/AC:L/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

CVSS v3 Base0020Score: 6.1

CVSS v3 Temporal Score 5.5

CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C

CVSS v3 Link:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C

Corrective Action or Resolution

The vulnerabilities have been fixed in version 6.5

ABB recommends that customers upgrade at earliest convenience

Vulnerability Details

ABB is aware of security vulnerabilities identified in the above versions of CCLAS that can allow an authenticated user access to files on the local file system through a Path Traversal flaw. By appending a local file path to a URL sent to /ria/file, an attacker can gain read access to the local file system. This can potentially allow read access to files with sensitive information. The application also contains a feature that will allow a user to configure an RSS feed by supplying a valid URL. It is possible to provide a URL that points to the local file system and gain access to local files.

Note: a user would need valid authentication credentials in order to exploit these two issues.

A Cross Site Scripting vulnerability has also been discovered which can allow an unauthenticated user the ability to execute JavaScript in a victim's browser by appending JavaScript to a URL sent to /ria/dispatch. An attacker would need a victim to perform an action such as clicking a hyperlink or possibly opening an email attachment.

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.

Workarounds

No workarounds have been identified.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could gain access to sensitive data on the application server file system, or a user's client system.

What causes the vulnerability?
The vulnerabilities are caused by a lack of proper input validation.

What might an attacker use the vulnerability to do?
An attacker can potentially gain read access to files on the local file system. An attacker may also be able to gain control of a victim's browser or client system.

How could an attacker exploit the vulnerability?
An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. 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. 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 modifies the way the application accepts user input, and implements proper input validation.

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.

Acknowledgements

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

- None

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.