ABB DOC ID: 9AKK107492A6224
REVISION: B
DATE: 2019-07-15

CYBER SECURITY ADVISORY

Authentication Bypass Vulnerability in CCLAS and Ellipse

2019-003-PGGA-CCLAS

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

The following ABB products are affected:

CCLAS versions 6.5, 6.6 – including all maintenance and hot fix releases

Ellipse 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9 - including all maintenance releases

Ellipse 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6

Vulnerability ID

ABB ID: 2019-003-PGGA-CCLAS

Summary

ABB is aware of a vulnerability in the product versions listed above. An attacker who successfully exploited this vulnerability could gain unauthorized access to report data within the CCLAS application.

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: 7.5 High

CVSS v3 Temporal Score: 6.7 Medium

CVSS v3 Vector: CVSS:3.0/AV:N/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:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Recommended immediate actions

The problem is corrected in the following product versions:

CCLAS 6.6.0.4 and 6.7

Ellipse 8.5.28*

Ellipse 8.6.25, 8.7.23, 8.8.19, 8.9.19, 9.0.7

ABB recommends that customers upgrade to the newest version at their earliest convenience.

Vulnerability Details

A vulnerability exists in the reporting mechanism for both CCLAS and Ellipse. When a report is generated it is stored on disk, and a URL is created to access the report through the UI. The URL request does not go through proper checks to ensure the user performing the request is an authenticated user. Anyone with access to the URL is able to download the report.

Mitigating Factors

Recommended security practices and firewall configurations can help protect an organization prevent attacks that originate from outside the network. Such practices include that 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. Any ports that are exposed to an untrusted external network should be evaluated case by case, justified and documented. Systems that process or store sensitive data 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

The following procedure can be used until an updated software version has been applied.

Issue Description:

- An attacker who is able to obtain a valid file download URL (e.g. http://www.example.com/ria/file?id=FileName.PDF&group=ReportFileGroup&type=PDF&refresh=ABCDEF01-2345-6789-ABCD-EF0123456789&fileHandler=file), will be able to download the report file even without login to the system.

Resolution:

1. Download the "**RIAWar.war**" file from the online application (batch, or both combined) server. Normally, the WAR file will be located in "`/opt/<product_name>/jboss/standalone/deployments/<EAR_Filename>" folder`
2. Extract the "**web.xml**" from the "**WEB_INF**" folder of the "**RIAWar.war**" package file
3. Add the line highlighted in yellow below:

[web.xml]

```
:
 <filter>
  <filter-name>authenticationFilter</filter-name>
  <filter-class>org.springframework.web.filter.DelegatingFilterProxy</filter-class>
 </filter>
:
 <filter-mapping>
```

```
    <filter-name>authenticationFilter</filter-name>
    <url-pattern>/remoteFile/*</url-pattern>
    <url-pattern>/spring/*</url-pattern>
    <url-pattern>/file</url-pattern>
  </filter-mapping>
:
```

4. Inject the amended "web.xml" into the "**RIAWar.war**" file using 7zip by replacing the same file in the exact location
5. Stop Jboss Web Application service (you need to have root access to do this) and backup the original "**RIA-War.war**" file in a safe location.
6. Replace the "**RIAWar.war**" with one produced from Step #3 and #4 above. Make sure the "**RIAWar.war**" file is owned by appliance:cloud.
7. Start Jboss Web Application service
8. Using a new browser (e.g. Chrome Private browser to avoid retrieval from local cache content) to access the URL highlighted above without login to the system, you should get the following page returned instead:

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who has access to the report download URL could gain access to report data without being authenticated to the application.

What causes the vulnerability?

The vulnerability is caused by insufficient authentication checks when accessing the URL for report download.

What is the affected product?

CCLAS versions 6.5, 6.6 - including all maintenance and hot fix releases

Ellipse 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9 - including all maintenance releases

Ellipse 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability would be able to access data included in reports without being authenticated to the application.

How could an attacker exploit the vulnerability?

An attacker would need to have access to the exact URL to download the report. This information could be obtained by intercepting the data sent across a network, or by gathering the URL from an authenticated user and altering the URL parameter values to access other reports.

Could the vulnerability be exploited remotely?

Yes, an attacker with network access to the web user interface would be able to exploit this vulnerability.

What does the update do?

The update remediates the issue by validating the web session identifier provided by the browser in the HTTP request header to determine whether an authenticated session has been established. If the web session identifier is not authenticated, the request will route to an error page.

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

None.

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.