Ellipse v8 Local File Inclusion Vulnerability

ABBVU-PGGA-201702

Update Date:

Notice

Affected Products

Ellipse 8.3 – 8.9

Vulnerability ID

ABB ID: ABBVU-PGGA-201702

Summary

ABB has received reports of a security vulnerability affecting the Ellipse application. An RSS function can be exploited to access files on the local file system.

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.

CVSS v2 Base Score: 6.8

CVSS v2 Temporal Score: 5.3

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 v3 Vector: 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

Corrective Action or Resolution

ABB has verified this issue and released a patch that removes the RSS functionality and provides checks to prevent URI's from accessing the local file system.

The following Ellipse versions have been created to address the issue reported in this security advisory:

Ellipse 8.4.34 released 30 March 2018

Ellipse 8.5.27 released 30 March 2018

Ellipse 8.6.22 released 6 April 2018.

Ellipse 8.7.18 released 7 Dec 2017 (includes update for Cyber Security Advisory Ellipse201703).

Ellipse 8.8.12 Released 7 Dec 2017 (includes update for Cyber Security Advisory Ellipse201703).

Ellipse 8.9.6 released 7 Dec 2017 (includes update for Cyber Security Advisory Ellipse201703).

Version Ellipse 8.3 of Ellipse is in sustaining support, customers will receive the resolution when and upgrade to Ellipse 8.x is planned.

ABB strongly recommends that customers apply the update as soon as they are able.

Vulnerability Details

The application contains functionality to allow users to configure RSS feeds by supplying a valid URL. By providing a URL that points to the local file system, a user is potentially able to gain access to sensitive data. This is due to improper validation of user input.

Mitigating Factors

A successful attack requires a user to be able to successfully authenticate to the application. A strong defense in depth security program that limits physical and logical access to the network can significantly reduce that attack surface. User awareness training is also important to ensure users understand the implications and risks associated with access to data.

Workarounds

No work arounds have been identified at this time.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could gain read access to files on the local file system, including sensitive system files.

What causes the vulnerability?
The vulnerability is caused by improper validation of URL's used as input into the application.

What is the affected product?
Ellipse v8.

Could the vulnerability be exploited remotely?
An attacker with access to the web interface and valid authentication credentials would be able to exploit this vulnerability

What does the update do?
The update removes the RSS functionality.

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

Support

For additional information and support please contact your local ABB service organization. For contact information, see

http://new.abb.com/enterprise-software/services/maintenance/support.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.