HITACHI ABB

Cybersecurity Advisory

Vulnerabilities in Hitachi ABB Power Grids Ellipse EAM

CVE-2021-27414

CVE-2021-27416

Notice

Affected Products and versions

Cross site scripting (CVE-2021-27416)

– affects Ellipse EAM versions prior to and including 9.0.25

Clickjacking (CVE-2021-27414)

– affects Ellipse EAM versions prior to and including 9.0.22

Vulnerability ID

CVE ID: CVE-2021-27414

CVE ID: CVE-2021-27416

Summary

An update is available that resolves a privately reported vulnerability in the product versions listed above.

An attacker who successfully exploited these vulnerabilities may be able to steal sensitive information, hijack a user's session, or compromise authentication credentials.

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.

Cross Site Scripting

CVSS v3 Base Score:	5.5
CVSS v3 Temporal Score:	5.0
CVSS v3 Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L/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:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

Clickjacking

CVSS v3 Base Score:	5.5
CVSS v3 Temporal Score:	5.0
CVSS v3 Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L/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:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

Vulnerability Details

Two vulnerabilities have been discovered in the Ellipse EAM web application front end included in the product versions listed above. In the case of Cross Site Scripting, an attacker could exploit these vulnerability by tricking a user to click on a link containing malicious code that would then be run by the browser. This can result in the compromise of confidential information, or even the take over of the user's session.

In the case of Clickjacking, an attacker can trick a user into visit a malicious web site posing as a login page for the Ellipse application and gather authentication credentials.

Recommended immediate actions

The problem is corrected in the following product versions:

- Cross Site Scripting (CVE-2021-27416) is fixed in Ellipse EAM version 9.0.26
- Clickjacking (CVE-2021-27414) is fixed in Ellipse EAM version 9.0.23

Hitachi ABB Power Grids recommends that customers apply the update as soon as they are able.

Mitigation Factors

Recommended security best practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include ensuring critical applications and 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. Firewalls should be configured to have the minimum number of ports exposed and open ports should be justified and documented. Critical 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. It is important to implement robust security awareness training to ensure users are able to identify common attacks or content such as phishing emails or malicious web pages.

Workarounds

No workaround have been identified.

Frequently Asked Questions

What is the scope of the vulnerability?

The vulnerabilities affect all users of the Ellipse EAM application.

What causes the vulnerability?

The vulnerability is caused by a lack of proper input validation and missing secure HTTPS headers.

What is the Ellipse application?

Ellipse is an EAM solution that manages the business processes and data from Assets, Works Management, Materials, Finance and Payroll/HR functions within capital intensive organizations. Ellipse EAM provides enterprise-wide management of assets in transportation, utilities and mining; its detailed equipment, project & costing models create the basis for asset lifecycle management & resource planning.

What might an attacker use the vulnerability to do?

An attacker may be able to steal sensitive information, hijack a user's session, or compromise authentication credentials.

How could an attacker exploit the vulnerability?

In the case of Cross Site Scripting, an attacker could exploit these vulnerability by tricking a user to click on a link containing malicious code that would then be run by the browser. This can result in the compromise of confidential information, or even the take over of the user's session.

In the case of Clickjacking, an attacker can trick a user into visit a malicious web site posing as a login page for the Ellipse application and gather authentication credentials.

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 ensuring critical 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 updates add the X-frame-options HTTP header to prevent Clickjacking, and sanitize user supplied input to prevent Cross Site Scripting.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, Hitachi ABB Power Grids received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had Hitachi ABB Power Grids received any reports that this vulnerability was being exploited?

No, Hitachi ABB Power Grids had not received any information indicating that this vulnerability had been exploited when this security advisory was originally reported.

Support

For additional information and support please contact your product provider or Hitachi ABB Power Grids service organization. For contact information, see https://www.hitachiabb-powergrids.com/contact-us/ for Hitachi ABB Power Grids contact-centers.