Stored XSS vulnerability in Ellipse APM

CVE-2021-27887

Notice

Affected Products and versions

Ellipse APM versions 5.3.0.1 and earlier

Ellipse APM versions 5.2.0.3 and earlier

Ellipse APM versions 5.1.0.6 and earlier

Vulnerability ID

CVE ID: CVE-2021-27887

Summary

A stored XSS vulnerability in the main dashboard of Ellipse APM versions prior to 5.3.0.1, 5.2.0.3, and 5.1.0.6 allows an authenticated user or integrated application to inject malicious data into the application that can then be executed in a victim's browser.

An update is available that resolves this internally reported vulnerability in the supported product versions listed above.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. 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 v3.1 Base Score:	6.3 (Medium)
CVSS v3.1 Temporal Score:	6.2
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:F/RL:U/RC:C
CVSS v3.1 Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:F/RL:U/RC:C&version=3.1

Vulnerability Details

A vulnerability exists in the main dashboard included in the product versions listed above. An attacker could exploit the vulnerability by creating/altering asset nameplate data to insert and run arbitrary code via eternally provided (stored) data which is directly used as part of the HTML code of the chart items tool tip.

Recommended immediate actions

The problem is corrected in the following product versions:

Ellipse APM versions 5.3.0.2, 5.2.0.4, and 5.1.0.7.

Hitachi ABB Power Grids recommends that customers apply the update at the earliest convenience.

Mitigation Factors

In general, applying cybersecurity hygiene will reduce the exploitation risk. The followings are some possible mitigation factors, namely:

– Ensure that the “Administrator” application role is only granted to fully trusted APM users – who are trained not to import harmful data to APM (e.g. containing HTML or JavaScript).

– Limit all “Import” role API credentials and integrations to only those providing safe data. Introduce filters in the source applications to ensure data safety.

– Introduce a Web Application Firewall solution in front of the APM-s web interfaces that has a capability of blocking XSS attack payloads in HTTP(S) requests, both plain REST (JSON/Xml) as well as Excel files wrapped in REST (JSON).

Workarounds

No workaround available.

Frequently Asked Questions

What is the scope of the vulnerability?

The vulnerability is limited to Ellipse APM application regular web UI, to a single component of the application main dashboard.

The web UI version for the mobile devices is not affected.

Only users interacting with the affected component could fall victim (or be a vessel of) an attack exploiting this vulnerability.

What causes the vulnerability?

The vulnerability is caused by lack of sanitization or proper encoding of user supplied application data, when shown via the affected component.

What might an attacker use the vulnerability to do?

A successful exploitation of this vulnerability could allow the attacker to take over a user’s session or compromise the confidentiality of information. It may also allow the attacker to affect the availability of the application.

How could an attacker exploit the vulnerability?

An attacker with Administrator privilege could try to exploit the vulnerability by injecting a specially crafted message into the application that could then be executed in a victim’s browser. This can be done by accessing the Ellipse APM’s web UI, or for an alternate integration scenario, injecting a specially crafted message via another system in the network that is connected to APM.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system (Ellipse APM or a data source system) could exploit this vulnerability. (See “How could an attacker exploit the vulnerability?”).

What does the update do?

The update removes the vulnerability by modifying the way that the application data is processed in the bar chart component, so it is properly encoded by dedicated safe library functions.

The provided data is no longer treated as part of the application HTML code, so is no longer executed, when the users are interacting with the component.

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

No, Hitachi ABB Power Grids received information about this vulnerability through internal processes.

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 issued.

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.