eSOMS Report Function Vulnerability

CVE-2021-26845

Notice

Affected Products and versions

eSOMS version 6.0 prior to 6.0.4.2.2

eSOMS version 6.1 prior to 6.1.4

eSOMS versions prior to 6.3

Vulnerability ID

CVE ID: CVE-2021-26845

Summary

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

An attacker who successfully exploited this vulnerability could gain access to unauthorized information.

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 pro-vided 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
CVSS v3 Temporal Score	:	6.7
CVSS v3 Vector	:	AV:N/AC:L/PR:N/UI:N/S:U/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:U/C:H/I:N/A:N/E:P/RL:O/RC:C
NVD Summary Link	:	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26845

Vulnerability Details

A vulnerability exists in the eSOMS reporting function that could allow an unauthorized user to gain access to report data if the URL used to access the report is discovered.

Recommended immediate actions

The problem is corrected in the following product versions:

eSOMS version 6.0.4.2.2

eSOMS version 6.1.4

eSOMS version 6.3

Hitachi ABB Power Grids recommends that customers apply the update as soon as possible.

Mitigation Factors

Recommended security practices and firewall configurations can help protect an organization network from attacks that originate from outside the network. Such practices include ensuring critical 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 that has a minimal number of ports exposed, and others that have to be evaluated case by case. 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.

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 unauthorized access to report data.

What causes the vulnerability?

The vulnerability is caused by insufficient authentication protections for report functionality

What is the eSOMS Reporting Feature?

eSOMS reporting feature allows users to run reports on eSOMS data.

What might an attacker use the vulnerability to do?

An attacker or unauthorized user who discovers the report URL would be able to gain access to that report.

How could an attacker exploit the vulnerability?

An attacker or unauthorized user who discovers the report URL would be able to gain access to that report.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability.

What does the update do?

The update implements checks to ensure the request is from an authenticated source and originates from the eSOMS application.

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 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.