REVISION: B
DATE: 2021-07-29
DOC. NUMBER: 9AKK107992A0957

CYBERSECURITY ADVISORY

Password Autocomplete Vulnerability in Hitachi ABB Power Grids eSOMS Application

CVE-2021-35527

Notice

The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi ABB Power Grids. Hitachi ABB Power Grids 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 Hitachi ABB Power Grids 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 Hitachi ABB Power Grids 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 Hitachi ABB Power Grids 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 and Versions

List of affected products and product versions:

– eSOMS version 6.3 or earlier

Vulnerability ID

CVE-2021-35527

Summary

Hitachi ABB Power Grids is aware of a privately reported vulnerability in the eSOMS product versions listed above. An update is available that resolves the issue which is described below.

An attacker who successfully exploited this vulnerability could gain access to user credentials that are stored by the browser.

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.

CVE-ID	Severity, Vector and Link to NVD[1]
CVE-2021-35527 - Password Field with Auto-Complete Enabled	CVSS v3.1 Base Score: 7.5 / High CVSS v3.1 Temporal Score : 7.0 / High CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C Link to NVD: click here

Vulnerability Details

The following vulnerability has been discovered in the eSOMS web application.

Password auto-complete enabled – the web application password field allows a browser to store user credentials. Stored passwords could be captured by an attacker who gains control over the users' system, or successfully exploits a Cross Site Scripting vulnerability in another application.

Recommended Immediate Actions

The problem is corrected in the following product versions:

Affected Version	Corrected Version
eSOMS versions 6.3 and prior	eSOMS version 6.3.1

[1] CVSS v3.1 Base Score, Temporal Score and Vector are updated in RevB of this document.

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

Mitigation Factors/Workaround

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 E-Mails or malicious web pages.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could gain access to user credentials that are stored by the browser.

What causes the vulnerability?

The vulnerability is caused by a lack of input control to prevent password caching.

What is the affected product?

The Hitachi ABB Power Grids eSOMS application can be used to manage the operations and shift schedule in a power plant.

What might an attacker use the vulnerabilities to do?

An attacker who successfully exploited this vulnerability could obtain a valid users' credentials in order to gain access to the application.

How could an attacker exploit these vulnerabilities?

An attacker can gain access to a users' password through a compromised client system or by exploiting a Cross Site Scripting vulnerability.

Could the vulnerabilities be exploited remotely?

Yes, the vulnerability can potentially be exploited by anyone with network access to the application interface.

What does the update do?

In eSOMS 6.3.1 the password control's property is modified to disable autofill of the password which will prevent it from being stored.

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 report 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.

Revision

Date	Revision	Description
2021-07-14	A	Original document
2021-07-29	B	Update on the Vulnerability Severity Section • Updated CVSS v3.1 Base Score 7.5 High • Updated CVSS v3.1 Temporal Score and Vector: 7.0 High • Updated CVSS v3.1 Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C