REVISION: A
DATE: 2021-08-05
DOC. NUMBER: 9AKK107992A5821

CYBERSECURITY ADVISORY

Password in Memory Vulnerability in Retail Operations Product

CVE-2021-35529

Notice

Affected Products and Versions

List of affected products and product versions:

Retail Operations version 5.7.2 and prior

Vulnerability ID

CVE ID: CVE-2021-35529

Summary

A vulnerability associated with a weakness in credential protection on the client environment of Retail Operations version 5.7.2 and prior allows an attacker, or an unauthorized user, who successfully exploits this vulnerability to access database credentials, shut down the product and access or alter system data.

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

Vulnerability Severity and Details

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	Detail Description
CVE-2021-35529 CVSS v3.1 Base Score: 7.7 High CVSS v3.1 Vector: /AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N Link to NVD: click here	A vulnerability exists in the product versions listed above. An attacker who has gained access to an authorized user's computer could exploit the vulnerability to access database credentials and gain read/edit access to the application data. This vulnerability is only exposed if an authorized user's computer has been accessed independently of the Retail Operations product.

Recommended Immediate Actions

The problem is corrected in the following product versions:

Affected Version	Corrected Version
Retail Operations v5.7.2 (and prior)	Retail Operations v5.7.3

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

Mitigation Factors and Workarounds

Recommended security practices, Operating Systems hardening, and firewall configurations can help protect a user's computer from the attacks. An entry point for this vulnerability is the unsecured Operating System on which the product is installed. We recommend hardening the Operating System accordingly. One recommendation is to follow the hardening guidelines published by "The Center for Internet Security (CIS)" https://www.cisecurity.org/about-us/

More information on the CIS recommended practices can be found in the following documents:

- CIS Benchmark v1.11.0-07-16-2021 for Microsoft Windows 10 Operating System https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

Each recommendation within a CIS Benchmark is assigned a Level 1 or Level 2 profile. Each organization may choose which recommendation to implement based on the organization cybersecurity requirements.

Additional hardening guidelines or CIS Benchmarks are published for Microsoft Office, Microsoft 365, Google Chrome, Microsoft Web Browser at https://www.cisecurity.org/cis-benchmarks/

Routinely monitor the application process log for unrecognized user sessions originating from outside the Retail Operations application.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could obtain unauthorized access to the application database.

What causes the vulnerability?

The vulnerability is caused by a weakness in the credential protection on the client environment.

What is Retail Operations?

Retail Operations is a software system used by utilities and energy marketers to: estimate load and generation; aggregate load and generation meter data; perform scheduling and energy accounting functions; communicate with market operators; perform wholesale billing and settlement functions.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could obtain unauthorized access to the database schema. With that information, an attacker could access/remove system data or render the system inoperable.

How could an attacker exploit the vulnerability?

To exploit the vulnerability, it requires the attacker to first obtain access the user computing environment and network credentials.

Could the vulnerability be exploited remotely?

Yes, if the remote desktop is setup on the operating systems that allow access to the computer remotely. an attacker that has gained access to a user’s computer could exploit the vulnerability.

What does the update do?

The update remediates completely the vulnerability.

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.