REVISION: A
PUBLICATION DATE: 2021-11-04
DOC. IDENTIFIER: 8DBD000067
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Authentication Bypass Vulnerability in Hitachi Energy Retail Operations Product

CVE-2021-35528

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of private reports of a vulnerability in the Retail Operations versions listed below. A flaw in the application authentication and authorization allows an attacker to execute a modified signed Java Applet JAR file. An attacker who successfully exploited this vulnerability could extract data or do modification of data inside Retail Operations.

An update is available that resolves the reported vulnerability.

Affected Products and Versions

List of affected products and product versions:

Retail Operations version 5.7.3 and prior

Vulnerability ID, Severity and Details

The vulnerability's severity assessment is performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1. The CVSS Environmental Score, which can affect the final vulnerability severity score, is not provided in this advisory as it reflects the potential impact of the vulnerability in the customer organizations' computing environment. Customers are recommended to analyze the impact of the vulnerability in their environment and calculate the CVSS Environmental Score.

Vulnerability ID	Detail Description
CVE-2021-35528 CVSS v3.1 Base Score: 7.2 High CVSS v3.1 Vector: AV:L/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. A flaw in the application authentication and authorization mechanism that depends on local validation of the session identifier allows an unauthorized modified signed Java Applet JAR file to be executed

Recommended Immediate Actions

The Table below shows the affected version and the recommended immediate actions.

Affected Version	Recommended Actions
Retail Operations v5.7.3 (and prior)	Retail Operations v5.7.3.1

Hitachi Energy recommends that customers apply the update at the earliest convenience.

General Mitigation Factors/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 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 data and do unauthorized modification on data inside Retail Operations.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by first gaining access to the underlying Operating System on which Retail Operations is installed. And then, Java expertise is also required to get the executable and modify it accordingly. Thus, if the underlying OS is not secured accordingly, the vulnerability can be exploited.

Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, if remote desktop function is enabled on the Operating System where the product is installed, an at-tacker may try to gain access via remote desktop functionality. Exploitation of this vulnerable is not bound to network stack.

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

No, Hitachi Energy received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had Hitachi Energy received any report that this vulnerability was being exploited?

No, Hitachi Energy 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 Energy service organization. For contact information, see https://www.hitachienergy.com/contact-us/ for Hitachi Energy contact-centers.

Publisher

Hitachi Energy PSIRT – cybersecurity@hitachienergy.com

Revision

Date of the Revision	Revision	Description
2021-11-04	A	Initial public release.