TLP:CLEAR
REVISION: 1
PUBLICATION DATE: 2023-09-08
DOC. IDENTIFIER: 8DBD000172
PUBLISHER: HITACHI ENERGY PSIRT
DOCUMENT STATUS: FINAL

HITACHI
Inspire the Next

CYBERSECURITY ADVISORY

Tag Out Vulnerability in Hitachi Energy's Asset Suite 9 product

CVE-2023-4816

Notice

Hitachi Energy

Summary

Hitachi Energy is aware of a reported vulnerability that affects the Asset Suite product version 9 Equipment Tag Out, when configured with Single Sign-On (SSO) password validation in T214. This vulnerability can be exploited by an authenticated user performing an Equipment Tag Out holder action for another user.
Please refer to the Recommended Immediate Actions for information about the mitigation/remediation.

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-2023-4816 CVSS v3.1 Base Score: 6.9 MEDIUM CVSS v3.1 Vector: AV:N/AC:L/PR:H/UI:R/S:C/C:N/I:H/A:L Link to NVD: click here **CWE-287**: Improper Authentication	A vulnerability exists in the Equipment Tag Out authentication, when configured with Single Sign-On (SSO) with password validation in T214. This vulnerability can be exploited by an authenticated user performing an Equipment Tag Out holder action (Accept, Release, and Clear) for another user and entering an arbitrary password in the holder action confirmation dialog box. Despite entering an arbitrary password in the confirmation box, the system will execute the selected holder action.

Affected Product Versions & Recommended Immediate Actions

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

Affected Version	Recommended Actions
Asset Suite 9.6.3.11.1 and below and Asset Suite 9.6.4	Apply one of the described mitigation strategies: 1. Configure Asset Suite 9 with a different authentication method other than SSO. 2. Configure Asset Suite security to disallow holder actions to be taken on behalf of other employees by removing authorization for the following security events to all users: T214ACT, T214RLS, and T214CLR. 3. Set Equipment Tag Out preference 'C/O HOLDER PSWD' to 'N'. Hitachi Energy recommends that customers affected by this vulnerability should apply one of the provided mitigation methods until a fix has been delivered in a patch. *

*Upgrade to Asset Suite version that fixes the vulnerability when available – remediation is under development.

General Mitigation Factors/Workarounds

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

Frequently Asked Questions

What is Hitachi Energy Asset Suite?

Asset Suite EAM (Enterprise Asset Management) for conventional and nuclear power generation is specifically designed to address the unique challenges faced by power generation operations, driven by utility requirements and implemented by utility-experienced teams.

Asset Suite EAM enables standardizing and streamlining work processes to maximize worker productivity, and improves ROI on assets through increased availability, reduced planned outage time, and improved reliability.

How could the vulnerability be exploited, and impact caused?

An authorized and authenticated user in the system, could perform a holder action on T214 on behalf of another user despite entering an arbitrary password. This vulnerability can potentially pose a safety hazard, if the user holder action was carried out unintentionally.

Could the vulnerability be exploited remotely?

Yes, any user with the ability to use the system remotely and the proper Asset Suite security privileges to perform holder actions on behalf of other users can exploit the vulnerability.

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

No, this vulnerability was not publicly disclosed. Hitachi Energy received information about this vulnerability through a stakeholder.

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

No, at the date of this advisory publication Hitachi Energy had not received any information indicating that this vulnerability had been exploited.

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
2023-09-08	1	Initial public release.

DocuSigned by: