September 29, 2023

Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Hitachi Energy Asset Suite 9 vulnerability. The vulnerability affects Asset Suite: Versions 9.6.3.11.1 and prior and Asset Suite: Version 9.6.4.

Technical Details

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.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk.

Hitachi Energy recommends applying one the following mitigation actions until a fix has been delivered in a patch:

- Configure Asset Suite 9 with a different authentication method other than SSO.
- 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.
- Set Equipment Tag Out preference 'C/O HOLDER PSWD' to 'N'.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-4816
- ICSA-23-269-02 Hitachi Energy Asset Suite 9

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts