WorkstationST - Reflected XSS in iHistorian Data Display Tags|CVE-2022-37952

Summary

A reflected cross-site scripting (XSS) vulnerability exists in the iHistorian Data Display of WorkstationST (<v07.09.15) could allow an attacker to compromise a victim's browser. WorkstationST is only deployed in specific, controlled environments rendering attack complexity significantly higher than if the attack were conducted on the software in isolation. WorkstationST v07.09.15 can be found in ControlST v07.09.07 SP8 and greater.

CVSS

3.6 (GE applies CVSS v3.1 Environmental Score to account for architectural controls)

Impact

The successful exploitation of this vulnerability could enable malicious actors to compromise a victim's browser context.

Vulnerable

- WorkstationST versions prior to v07.09.15

Recommendation

Upgrade to Workstation >= 7.09.15 which can be found in ControlST 7.09.07c SP8 and greater.

Workaround

Customers should follow the guidance laid out in GEH-6839. The best practices described in that document limit the likelihood and impact of a wide variety of attacks.

GE Power Product Security Incident Response Team (PSIRT)

Providing secure and reliable products and solutions is vital to the operations of GE Gas Power. Our products are designed with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect our products and customers.

Contact Information

Contact your local GE Services representative for assistance or for additional information. For Product Security issues or incident/vulnerability reporting: www.ge.com/power/cybersecurity

Credit

GE Gas Power would like to thank Ammar Majali for his evaluation and responsible disclosure of this vulnerability.

Additional Resource(s)

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CVE-2022-37952

Document History

Version	Release Date	Purpose
1.0	8/24/2022	Initial publication