ToolboxST - Deserialization of Untrusted Configuration Data | CVE-2023-1552

Overview
GE Gas Power has been made aware of a vulnerability in ToolboxST versions prior to 7.10 as part of a vulnerability disclosure submitted by Claroty to GE Gas Power PSIRT. CVE-2023-1552 has been assigned to this vulnerability.

Vulnerability Details
ToolboxST versions prior to version 7.10 are affected by a deserialization vulnerability. An attacker with local access to an HMI, or who has conducted a social engineering attack on an authorized operator, could execute code in a Toolbox user's context through the deserialization of an untrusted configuration file.

Affected Products and Versions
ToolboxST versions < 7.10

Severity Assessment
CVSS 2.9 (Low) – Attacker with local access to HMI
CVSS 6.4 (Medium) – Social engineering attack on authorized operator

Exploitation Status
GE Gas Power is not aware of any attempt to exploit this vulnerability in customer equipment.

Remediation
Customers are advised to update to ToolboxST 7.10 which can be found in ControlST 7.10. If unable to update at this time, customers should ensure they are following the guidance laid out in GE Gas Power's Secure Deployment Guide (GEH-6839). Customers should ensure they are not running ToolboxST as an Administrative user.

Acknowledgements
GE Gas Power would like to thank Sharon Brizinov of Claroty for discovering and disclosing this vulnerability to our Product Security team.

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 engineered 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

Document History

Version	Release Date	Purpose
1.0	March 23rd, 2023	Initial release