# Vulnerabilities In ToolBoxST

## Overview

GE Gas Power became aware of several vulnerabilities in its ToolBoxST version v04.07.05C. Our Controllers use ToolboxST as a software platform for programming, configuring I/O, trending, and analyzing diagnostics. At the controller level and at the facility level, it allows for the effective management of equipment with increased reliability and time-synchronized data. Failure to apply the remediations provided below may create risk of information disclosure and remote code attack execution.

## Affected Product and Version

All ToolBoxST OS versions prior to 07.09.07C are affected by this Security Advisory.

## Vulnerability Details

**Improper Restriction of XML External Entity Reference (CWE-611)**

CWE-611 refers to vulnerabilities that arise when an application processes an XML document that contains entities referring to external URIs. These URIs resolve to assets outside the control of the application, resulting in the potential data exfiltration.

GE Gas Power ToolBoxST version v04.07.05C suffers from an XML External Entity (XXE) vulnerability using the DTD parameter entities technique that can result in disclosure and retrieval of arbitrary data on the affected node via out-of-band (OOB) attack. The vulnerability is triggered when input passed to the xml parser is not sanitized while parsing the xml project/template file.

## Severity Assessment:

Low

## Exploitation Status

GE Gas Power Product Security is not aware of any malicious attempts to exploit this vulnerability.

## Workarounds and Mitigations

The ToolBoxST OS version 07.09.07C and above has fixed this issue by disabling the use of DTD’s, which are not necessary for ToolBoxST functionality.

**Vulnerability #2: Improper Limitation of a Pathname to a Restricted Directory (CWE-22)**

CWE-22, also known as a path traversal vulnerability, refers to the ability of unauthorized parties to access restricted directories. Path traversal allows unauthorized users to access restricted directory files. Some of the files are benign, while others may provide unauthorized users with information that can be used to access more sensitive areas. In some cases, the malicious party may be able to modify the files it accesses. Engaging in a path traversal attack does not require any special tools; the malicious party only needs access to a web browser and the patience to sift through many directories to find files and directories of interest.

ToolBoxST prior to version 7.8.0 uses a vulnerable version of the Ionic .NET Zip library that does not properly sanitize path names such that files can be extracted to a location above their parent directory, all the way back to the root directory. If an attacker compromises an HMI or creates their own SDI client, they can upload the device.zip file from a controller, patch it to contain a malicious file and path, and download it back to the controller. The next user to perform an upload will grab the malicious device.zip and extract it to their HMI, creating the potential for arbitrary write, overwrite, and execution.

### Severity Assessment:

Low

### Exploitation Status

GE Gas Power Product Security is not aware of any malicious attempts to exploit this vulnerability.

### Workarounds and Mitigations

This is resolved as of ToolBoxST version 7.8.0 due to the upgrade of the Ionic library. Customers should ensure they are following the password protection and network segmentation guidance laid out in GEH-6839. Additionally, the use of SDI Secure Mode offers considerable protection against this attack as the threat actor must be able to perform a download to the controller over SDI. Secure Mode validates authenticity and protects against spoofing of SDI commands.

### Recommendations

GE Gas Power Cybersecurity and Engineering teams will continue to investigate internally as well as monitor industry-based news for any changes or updates. To reduce the risk that vulnerabilities like this may represent to the controls network, we recommend the implementation of a good defense- in-depth strategy as detailed in our GEH 6839 Secure Deployment Guide. Some of our recommended controls include:

- Minimize network exposure for all Controllers with the use of network segmentation, placement of controllers behind controls network firewalls and ensure that they are not accessible from the Internet.
- Block suspicious external IP addresses at the controls network firewalls. Monitor traffic internally for unusual behavior.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.
- Implement defense-in-depth within the controls network environment consisting of tools such as Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, and network access control (NAC).
- Implement and maintain an anti-malware solution and an endpoint detection and response (EDR) solution.
- Disable remote access services and protocols such as Remote Desktop Protocol (RDP) unless needed. Monitor and restrict remote access usage on a least-privilege basis.
- Have backup and restore processes and procedures in place for disaster recovery and incident response.

- Monitor and maintain account provisioning and access control based on the principle of least privilege

### Acknowledgement

We would like to acknowledge Sharon Brizinov and Noam Moshe of Claroty for helping to identify these vulnerabilities during a security assessment.

### 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. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.

### Additional Information

ICSA-22-025-01 GE Gas Power ToolBoxST
https://www.cisa.gov/uscert/ics/advisories/icsa-22-025-01

### Document History

| Version | Release Date | Purpose |
|---|---|---|
| 1.0 | November 9th, 2021 | ToolBoxST v04.07.05C. Vulnerability Assessment and Potential Product Impact Statement |
| 2.0 | January 20th, 2022 | Obtained CISA ID |
| 3.0 | February 7th, 2022 | Removed v04.07.05C from title Changed Naom Moshe to Noam Moshe |