WorkstationST EGD Configuration Server – Arbitrary File Overwrite

Overview

A pair of vulnerabilities impacting GE Vernova's WorkstationST – EGD Configuration Server were disclosed to GE Vernova by Ricardo Pelaz García and Roberto Garcia Hervás of Innotec Security part of Accenture.

Affected Products and Versions

WorkstationST V07.10.10C and earlier

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
ISSUE 1	9.4 (Critical)	5.8 (Medium)	WorkstationST	Unauthenticated file write (CWE-306)
ISSUE 2	9.4 (Critical)	5.8 (Medium)	WorkstationST	Path traversal (CWE-35)

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

Issue 1 would allow an unauthenticated user to write or overwrite files to the EGD Configuration Server, while Issue 2 does not properly escape paths from the upload field. Combined, these issues could enable an unauthenticated user to overwrite arbitrary files in any location within the EGD Configuration Server.

Exploitation Status

GE Vernova has not yet observed nor received reports of any compromise of Gas Power customer equipment due to these vulnerabilities.

Remediation/Mitigation

The path traversal issue is resolved in WorkstationST V08.00, as well as V07.10.11C. Customers should update their WorkstationST installation to one of these versions.

The ability to perform unauthenticated file upload is required for the proper operation of the EGD Configuration server. As such, this issue has not been addressed directly, but the removal of the path traversal issue will prevent an attacker from impacting the operational integrity of the equipment.

Additional Notes

GE Vernova would like to thank Ricardo Pelaz García and Roberto Garcia Hervás of Innotec Security part of Accenture, for reporting these vulnerabilities through our responsible disclosure process.

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information.
For Product Security issues or incident/vulnerability reporting: https://www.gevernova.com/security

Document History

Version	Release Date	Purpose
1.0	9/24/2024	Initial Release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.