GE Digital CIMPLICITY Memory Corruption | CVE-2023-3463

Overview

A GE Digital CIMPLICITY vulnerability was published on July 19th, 2023, under the ID CVE-2023-3463. It describes a heap-based buffer overflow vulnerability [CWE-122] in CIMPLICITY.

Severity

GE Digital has assigned a base CVSS v3 score of 6.6 (medium) to this vulnerability.

Affected Products and Versions

GE Digital CIMPLICITY

- All versions prior to CIMPLICITY 2023

Vulnerability Details

All versions of GE Digital CIMPLICITY that are not adhering to Secure Deployment Guide (SDG) guidance and accepting documents from untrusted sources are vulnerable to memory corruption issues due to insufficient input validation, including issues such as out-of-bounds reads and writes, use-after-free, stack-based buffer overflows, uninitialized pointers, and a heap-based buffer overflow. Successful exploitation could allow an attacker to execute arbitrary code.

Exploitation Status

GE Gas Power Product Security has not yet observed nor received reports of any exploit attempts against Gas Power Customers. Additionally, this vulnerability is not remotely exploitable; exploitation is only possible if an authenticated user with local access to the system obtains and opens a document from a malicious source.

Remediation/Mitigation

Due to the need for local authentication of a legitimate user to exploit, GE Gas Power holds that the actual risk of exploitation is low, given existing compensating controls and adherence to GE Digital's Secure Deployment Guide for CIMPLICITY. To minimize the risk of exploitation of this vulnerability, GE Gas Power recommends that customers maintain strong access control, avoid introduction of files to the system from unidentified or malicious sources, and adhere to the CIMPLICITY Secure Deployment Guide provided by GE Digital.

GE Gas Power is currently performing validation of CIMPLICITY 2023 to ensure compatibility with existing equipment and has not yet approved CIMPLICITY 2023 for deployment at Gas Power customer sites. GE Gas Power will update this advisory when the deployment of CIMPLICITY 2023 has been approved for use and upgrades are made to be commercially available through the GE Gas Power sales team.

Resources

CISA Disclosure
GE Digital Security Bulletin
GE Digital CIMPLICITY Secure Deployment Guide

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	8/10/2023	Initial Release