ICS Advisory (ICSA-20-098-02) for CIMPLICITY

Date: June 12, 2020

Overview

A local privilege escalation vulnerability CVE-2020-6992 (ICSA-20-098-02) identified on CIMPLICITY HMI (versions 10.0 and below). If exploited, the vulnerability could allow an adversary to modify the system leading to the arbitrary execution of code at a potentially higher privilege level.

Affected Products

GE Control Platform with CIMPLICITY versions 10.0 and below.

Recommendations

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- **Confidentiality**: Ensure only the people you want to see information can see it.
- **Integrity**: Ensure the data is what it is supposed to be.
- **Availability**: Ensure the system or data is available for use.

GE recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their GE products and solutions.

- Sites should review **TIL 1881-R2** for completeness to ensure that the system is well protected from any external attacks
- Consider Configuration Hardening by way of taking steps to reduce attack surfaces that may be used in an attack on the system which include removing functions that are not essential and changing system settings to help deter attacks. This could be achieved by following
    - **Disable unused Servers and Services on each device.**
    - **Create and maintain the list of users and their rights.** Disable or remove a user's account as soon as the person is no longer granted access rights to the equipment.
    - **Implement the site's password policies**, where possible by configuring the equipment to reject passwords that don't meet the standards automatically.
    - **Remove all as shipped accounts or (if the account is to remain) change all passwords as soon as feasible during the site commissioning process**. Implement strict site policy and controls to limit the exposure of passwords.

- This specific vulnerability can be exploited through unauthorized access to the program files directory where the CIMPLICITY software is loaded on the HMI Workstation or Server. GE and our authorized partners configure the hard drive where the program files directory is found such that only users with the Administrator role have write access to the drive (All directories mentioned in the %PATH% environment variable on the system have ACLs (Access Control Lists) set to prevent all users, except users in the administrators' group). This configuration reduces the risk of unauthorized users from accessing the system and exploiting this vulnerability.

References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6992
- https://www.us-cert.gov/ics/advisories/icsa-20-098-02
- https://www.ge.com/power/cybersecurity
- GEH-6839 (Please contact your local GE service representative for this document)
- TIL 2086

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.