Vulnerabilities In GE CIMPLICITY

Overview

As part of routine work with a long-term security partner, GE Digital recently identified, and proactively developed mitigation plans for two vulnerabilities in GE Digital's Proficy CIMPLICITY product. While this is a common process in the software industry, cybersecurity is GE Digital's top priority and the Engineering & Manufacturing teams have worked quickly to offer solutions to both issues.

The first issue requires a code fix that has already been implemented and released, while the second issue is resolved as a configuration item that is currently published in GE Digital's secure deployment guide.

Vulnerability Details

GE Digital Proficy CIMPLICITY Privilege Execution Vulnerability

GE Digital (GE) became aware of Privilege Execution vulnerabilities (Vulnerabilities) having the potential to impact its Proficy CIMPLICITY software (Affected Software). After assessing the Vulnerabilities for the Affect Software, GE determined the Vulnerabilities could be exploited to result in local privilege escalation and remote code execution. At this time, GE believes exploitation of the Vulnerabilities is only possible if the attacker has access to log into the machine running Proficy CIMPLICITY. An exploit may only be possible if the CIMPLICITY server is not already running a project and the server is licensed for multiple projects.

Affected Products and Versions

Proficy CIMPLICITY 11.1 and previous versions

Severity Assessment:

Low

Exploitation Status

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

Remediation / Fixes

GE strongly recommends users upgrade all instances of the Affected Software to GE Digital's Proficy CIMPLICITY, released January 2022 (Upgrade) and follow the instructions in the Secure Deployment Guide to restrict which CIMPLICITY projects are allowed to run. The Upgrade contains what GE believes are mitigation measures to help ensure the Vulnerabilities cannot be exploited.

Workarounds and Mitigations

None.

Other Recommendations

GE Digital believes the Upgrade is the most effective way to address the Vulnerabilities. Workarounds may mitigate some of the issues but only the Upgrade will fully address the identified Vulnerabilities. For those customers electing not to implement the Upgrade, GE Digital recommends applying the instructions in CIMPLICITY's Secure Deployment Guide to ensure access to the CIMPLICITY machines and directories are properly controlled via Access Control Limits (ACLs).

GE Digital Proficy CIMPLICITY Credentials Vulnerability
GE Digital (GE) became aware of credential vulnerabilities (Vulnerabilities) having the potential to impact its Proficy CIMPLICITY software (Affected Software). After assessing the Vulnerabilities for the Affected Software, GE determined the Vulnerabilities could be exploited to:

- Connect to HMI screens that the attacker access to
- Get information about alerts and draw conclusions about the systems
- Get CIMPLICITY points values and, in some cases, change them

At this time, GE believes exploitation of the Vulnerabilities is most likely to occur if the attacker has the ability to capture a connection session between a CIMPLICITY client of the Affected Software to the server.

Affected Products and Versions
Proficy CIMPLICITY

Severity Assessment:
Low

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

Remediation / Fixes
Users are strongly advised to refer to the Secure Deployment Guide (SDG) instructions on how to configure communication encryption. The complete SDG can be found at the link below. Login | GE Digital Customer Center. It is also recommended that users review the **CIMPLICITY Windows Hardening Guide and Recommendations** for further IPSEC configuration guidance found in the section titled Appendix A IPSEC Configuration.

Workarounds and Mitigations
None.

Additional Recommendations
None

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 22nd, 2022	Initial release
2.0	September 29th, 2022	

		Updated document classification details