

Proficy Historian Authentication, Access Control and File Upload Vulnerabilities | ICSA-23-017-01

Overview

GE Digital provided GE Gas Power advance notification regarding several Proficy Historian vulnerabilities that were ultimately disclosed through CISA on January 17th 2023.

Affected Product and Version

- This vulnerability impacts the Mark Vie Control System Historian via GE Digital's Proficy Historian
 - Proficy Historian versions ≥ 7 and < 2023
 - GPS Historian Windows OS version $\geq$ Windows Server 2012

Vulnerability Details

GE Digital became aware of Authentication, Access Control and File Upload vulnerabilities having the potential to impact its Proficy Historian Software.

After assessing the Vulnerabilities for the Proficy Historian Software, GE Digital determined that the below Vulnerabilities could be exploited to result in the following:

- Client can potentially bypass authentication while connecting to Historian Server
- Attacker may be able to authenticate and perform file operations on remote server machine
- Attacker may be able to view/change data while transferring between client/collector machine and server machine

GE Digital believes it has taken appropriate steps to address the Vulnerabilities in the most recent Historian 2023 release and GE Gas Power is in the process of validating the provided updates.

Exploitation Status

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

Mitigations

The following SIMs have been validated in our environment for each of the impacted versions of Proficy Historian. Please contact your local GE Services representative for support in receiving and installing the SIM listed below according to your version of Proficy Historian.

- Proficy Historian 7.1 SIM4
- Proficy Historian 8.1 SIM3
- Proficy 2022 SIM2

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	2/3/2023	Initial release
2.0	6/16/2023	Updated patch information