WOODWARD

GE Digital iFIX Vulnerability

Issue

Certain Woodward turbine control systems utilize GE Digital iFIX as a basis for the system HMI interface. GE Digital has been made aware of three Vulnerabilities affecting its HMI/SCADA iFIX v6.1 and earlier versions. If exploited, the Vulnerabilities could allow an attacker to modify the Affected Software system leading to arbitrary execution of code.

Description

- GE Digital believes the Vulnerabilities may result in privilege escalation permitting an attacker to access information and execute malicious code in a user's environment.

- If exploited, the vulnerabilities could allow an attacker to modify the user's system wide GE Digital iFIX configuration.

- GE Digital believes that this vulnerability is only exploitable if an attacker has system access.

- See CISA Advisory https://us-cert.cisa.gov/ics/advisories/icsa-21-040-01

- See GE Digital Advisory https://digitalsupport.ge.com/communities/en_US/Article/GE-Digital-Security-Advisory-GED-21-01?Type=Alert__kav

Affected Units

All HMIs and workstations running iFIX v6.1 and older.

Corrective Action

- GE Digital believes it has addressed the Vulnerabilities with the most recent release of GE Digital HMI/SCADA iFIX 6.5 on February 1, 2021.

- The iFIX Secure Deployment Guide includes recommendations securing iFIX files and registry entries on the HMI. This is not a replacement for upgrading to 6.5 but it can help reduce the risk that the vulnerability could be exploited until the upgrade can be completed.

Customer Action

- GE Digital recommends users immediately upgrade all instances of the Affected Software to GE Digital's iFIX product v6.5 released on February 1, 2021.

- The Upgrade contains security enhancements that GE Digital believes will mitigate the risk that the Vulnerabilities may be exploited by an attacker.

- Please contact your Woodward support resource about the option of upgrading your systems to 6.5.

- In addition to immediately installing GE Digital HMI/SCADA iFIX v 6.5, GE Digital advises users' adherence to the iFix Secure Deployment Guide found on GE Digital's Customer Center:

  https://digitalsupport.ge.com/communities/en_US/Documentation/iFIX-Secure-Deployment-Guide

- Adherence to the recommendations in section 3.2.2 of the Guide will help control user access and logins to the HMI and will reduce the risk the Vulnerability may be exploited. Contact your Woodward support resource if assistance is needed in implementing section 3.2.2.