GE Digital Product Security Advisory

Title:	GE Digital iFIX Vulnerabilities
Vulnerability ID:	GED 21-01
Other identifiers:	ICSA-21-040-01
Release date:	2/5/2021

Summary

GE Digital has been made aware of three vulnerabilities (Vulnerabilities) affecting its HMI/SCADA iFIX v6.1 and prior software (Affected Software).

If exploited, the Vulnerabilities could allow an attacker to modify the Affected Software system leading to arbitrary execution of code.

At this time, 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.

Further, GE Digital believes the Vulnerabilities may only be exploitable if an attacker has system access.

GE Digital believes it has addressed the Vulnerabilities with the most recent release of GE Digital HMI/SCADA iFIX 6.5 on February 5, 2021. Users of the Affected Software at risk for the Vulnerabilities are advised to upgrade the Affected Software immediately in accordance with the Solution below.

Affected software

GE Digital HMI/SCADA iFIX v6.1 and prior versions of the software

Solution

GE Digital recommends HMI/SCADA iFIX users upgrade all instances of the Affected Software to GE Digital's iFIX product v6.5 released on February 5, 2021 (Upgrade) and install using Secure Mode.

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

Please contact your GE Digital Channel representative or email gedclientservices@ge.com.

Other Recommendations

GE Digital advises users of HMI/SCADA iFIX to carefully adhere to the iFix Secure Deployment Guide (Guide) found on GE Digital's Customer Center:

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

The Guide provides manual steps to users of all versions of the software.

Adherence to the recommendations in the Guide, in addition to maintaining a comprehensive enterprise cybersecurity plan, is strongly recommended by GE Digital and at this time we believe the recommendations, when implemented properly by our customers and in accordance with this Advisory, will help reduce the risk the Vulnerability may be exploited by an unauthorized user.

Vulnerability information

The Vulnerability identified in the Affected Software, if exploited, could allow an attacker to modify the user's system-wide GE Digital iFIX configuration. The Vulnerability is only exploitable if an attacker has access to an authenticated session.

Thanks to researchers William Knowles with Applied Risk and Sharon Brizinov of Claroty and for bringing information about the Vulnerabilities to GE Digital's attention.

Disclaimer

Auto-Notification

Please visit the customer profile page on our support site to sign-up for auto-notifications for GE Digital products and services to receive immediate notice of security alerts and information.

Instructions on "How to sign up for Auto-Notifications for updates" can be found here

https://digitalsupport.ge.com/en_US/Article/How-to-sign-up-for-Auto-Notifications-for-GE-Digital-products

Change log

Date	Change(s)
February 5, 2021	Initial release
February 9, 2021	Updates to Other Identifiers, Release Date, Other Recommendations
February 22, 2021	Updates to Solution, Other Recommendations