GE Digital Product Security Advisory

Title:	Password Management Vulnerability
Vulnerability ID:	GED 16-02
Other identifiers:	ICSA-16-336-05
Release date:	11-29-2016
Last updated:	January 20, 2017
CVSS v3 Base Score	6.4 (Medium)

Summary

A password management vulnerability has been identified in the Proficy HMI/SCADA iFIX, Proficy HMI/SCADA CIMPLICITY and Proficy Historian products, that, if exploited, could allow an adversary to retrieve user passwords.

Proficy HMI/SCADA-CIMPLICITY, is a Client/Server-based HMI/SCADA application. Proficy Historian is a data historian that collects, archives, and distributes production information. According to GE, these products are deployed across multiple industries worldwide and sold by its GE Digital business, Automation and Controls business, and its resellers and distributors.

This vulnerability is only exploitable if an attacker has access to an authenticated session.

Affected software

- Proficy HMI/SCADA iFIX 5.8 SIM 13 and earlier versions
- Proficy HMI/SCADA CIMPLICITY 9.0 and prior versions
- Proficy Historian 6.0 and prior versions

Solution

Installing the following versions and/or SIM (or any later version or SIM) will address this issue:

- GE HMI/SCADA CIMPLICITY 9.5
- GE CIMPLICITY 8.2 SIM 49
  https://ge-ip.force.com/communities/en_US/Download/CIMPLICITY-8-2-SIM-49
- GE CIMPLICITY 9.0 SIM 22
  https://ge-ip.force.com/communities/en_US/Download/CIMPLICITY-9-0-SIM-22
- GE Historian 7.0
- Historian 6.0 SIM9
  https://ge-ip.force.com/communities/en_US/Download/Historian-Standard-6-0-SP1-SIM-9
  https://ge-ip.force.com/communities/en_US/Download/Historian-Enterprise-6-0-SP1-SIM-9
- Historian 5.5 SIM37
- https://ge-ip.force.com/communities/en_US/Download/Historian-5-5-SIM-37

- GE HMI/SCADA iFIX 5.8 SIM 14
  https://digitalsupport.ge.com/communities/en_US/Download/iFIX-5-8-Service-Pack-2
- GE HMI/SCADA iFIX 5.5 SIM due February 28, 2017. iFIX customers with versions earlier than iFIX 5.5 who can't upgrade should contact GE Support.
- To obtain the latest versions of these products please contact your local GE Digital representative. Contact information is available at https://digitalsupport.ge.com/communities/CC_Contact

Other Recommendations

GE Digital recommends that all customers upgrade to GE HMI/SCADA CIMPLICITY 9.5. Workarounds may mitigate issues but only upgrading will fully address an issue.

For users unable to upgrade to GE HMI/SCADA CIMPLICITY 9.5, the following steps may mitigate the risks described above:

1) Enable project configuration security and limit the number of users that have access to the workbench to only those that need to configure the project.

2) Enable Windows domain authentication so that CIMPLICITY users' passwords are not stored in CIMPLICITY.

Vulnerability information

The vulnerability identified in the iFIX, CIMPLICITY, Historian products, if exploited, could allow an adversary to retrieve user passwords. This vulnerability is only exploitable if an attacker has access to an authenticated session.

Thanks to researcher Ilya Karpov of Positive Technologies for bringing this matter to GE Digital's attention.

Disclaimer

Product advisories provided here are subject to terms and conditions contained in customers' underlying license agreements or other applicable agreements. Due to ongoing product enhancements, GE reserves the right to change or update advisories without advance notification.

Auto-Notification

Please visit the customer profile page on the support site to sign up for auto-notifications for GE Digital products in order 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/communities/en_US/Article/How-to-sign-up-for-SIM-Auto-Notification-for-GE-Intelligent-Platforms-software-products-KB12680-en-US

Change log

Date	Change(s)
October 4, 2016	Initial release
November 28, 2016	ICS-CERT ICSA# & Publication Date, Summery, Contact URL
December 14, 2016	Other Recommendations
January 20, 2017	Updated ICS Cert reference to ICSA-16-336-05
February 13 2017	Additional SIM information
May 8, 2017	Additional SIM information