GE Intelligent Platforms Product Security Advisory

Title: Multiple vulnerabilities in Proficy HTML Help
Vulnerability ID: GEIP12-04
Other identifiers: KB14863, ZDI-CAN-1491, Bugtraq ID 36546
Release date: April 24, 2012
Last updated: August 21, 2018

August 2018 - Users may have received recent Twitter notifications stemming from a correction to broken links with ICS-Cert . There is no new information or changes to 2012 report below.

Summary

Multiple vulnerabilities have been discovered in the third-party HTML Help functionality used by some versions of Proficy Historian, Proficy HMI/SCADA – iFIX, Proficy Pulse, Proficy Batch Execution, and the SI7 I/O Driver. If an attacker tricks a user into visiting a malicious website, these vulnerabilities could potentially allow the attacker to execute arbitrary code on the client or could potentially allow the attacker to place or replace files on the client.

GE Intelligent Platforms recommends that customers remove the vulnerable ActiveX control to eliminate the vulnerability. GE Intelligent Platforms has provided a removal tool to assist customers with this process.

In addition, GE Intelligent Platforms has released a product update for Proficy Historian to remove that product's dependency on the vulnerable control.

Affected software

- Proficy Historian: Versions 4.5, 4.0, 3.5, and 3.1
- Proficy HMI/SCADA – iFIX: Versions 5.1 and 5.0
- Proficy Pulse: Version 1.0
- Proficy Batch Execution: Version 5.6
- SI7 I/O Driver: Versions between 7.20 and 7.42 (Version 7.42a does not install the control)

Note: Although Proficy HMI/SCADA – iFIX Version 5.5 does not install the vulnerable control, customers who have upgraded to 5.5 from version 5.1 or 5.0 should follow the vulnerability removal instructions.

Solution

Vulnerability removal instructions

IMPORTANT: The KeyHelp.ocx ActiveX control must be unregistered to eliminate the vulnerability. GE Intelligent Platforms recommends unregistering and also deleting the control. The SIMs below ensure that Proficy Historian software functions properly once the control is removed.

1. Obtain keyhelpremoval.bat from KB14863 at http://support.geip.com/support/index?page=kbchannel&id=S:KB14863
2. Run keyhelpremoval.bat as a user in the Administrators group
3. Navigate to the "System32" directory (or the "Syswow64" directory on 64-bit systems) of your Windows installation and verify that KeyHelp.ocx no longer exists

The batch file runs the following commands to unregister and delete the control. This procedure can also be performed manually – for example, from the command line:

```
%SystemDrive% cd %SystemRoot%/syswow64 if
EXIST Keyhelp.ocx regsvr32 -u Keyhelp.ocx
erase keyhelp.ocx

%SystemDrive% cd %SystemRoot%/System32 if
EXIST Keyhelp.ocx regsvr32 -u Keyhelp.ocx
erase keyhelp.ocx
```

Additional steps required for Historian installations

The vulnerable control is installed with the Historian Administrator client, which is also installed on the server. If the vulnerable control is removed prior to the SIM being installed, Proficy Historian Administrator may crash if the user presses F1 for Help.

The following product updates address this issue:

- Proficy Historian 4.5 SIM 7 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3811
- Proficy Historian 4.0 SIM 19 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3778
- Proficy Historian 3.5 SIM 19 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3820
- Proficy Historian 3.1 SIM IH31_11465436841.exe at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3824

Note: These SIMs remove dependency on the vulnerable component – the removal tool must be run to address the vulnerability. Proficy SIMs are cumulative. All future SIMs will include these updates. **iFIX installations**

The vulnerable control is installed with both the client and the server. Running the removal tool eliminates the vulnerability. No SIM is required.

Pulse installations

The vulnerable control is installed with the Proficy Pulse client. Running the removal tool eliminates the vulnerability. No SIM is required.

SI7 I/O Driver installations

The vulnerable control is installed with the I/O Driver. Running the removal tool eliminates the vulnerability. No SIM is required.

Vulnerability information

A remote stack-based buffer-overflow condition exists in the KeyHelp.ocx control because it fails to perform adequate boundary checks on user-supplied input.

In addition, a remote command injection vulnerability exists in the KeyHelp.ocx control because it fails to restrict or perform adequate validation on user-supplied input.

Acknowledgements

GE Intelligent Platforms would like to thank Andrea Micalizzi aka rgod and the Zero Day Initiative for reporting this issue in Proficy Historian.

GE Intelligent Platforms performed an analysis that identified and addressed the same issue in additional products.

Change log

Date	Change(s)
April 25, 2012	Added a link to the Historian 3.1 SIM
May 11, 2012	Added information on 64-bit installations. Re-posted keyhelpremoval.bat to account for 64-bit installations.
August 18, 2018	Notification of fixing broken links