GE Intelligent Platforms Product Security Advisory

Title: Memory corruption in Proficy Historian ihDataArchiver
Vulnerability ID: GEIP12-01
Other identifiers: KB14767, CVE-2012-0229, ICS-VU-519897, ZDI-CAN-1377
Release date: January 31, 2012
Last updated: March 12, 2012

Summary

A vulnerability exists in Proficy Historian that, if exploited, could allow an attacker to cause the Historian Data Archiver service to crash or potentially take control of a system running the affected software.

GE Intelligent Platforms recommends that customers apply product updates to Proficy Historian versions 3.1, 3.5, 4.0, and 4.5. Proficy Historian customers using versions older than 3.1 are encouraged to upgrade to 3.1 or greater and then apply the appropriate product update.

GE Intelligent Platforms also recommends that Proficy HMI/SCADA – iFIX and Proficy HMI/SCADA – CIMPLICITY customers who have installed Proficy Historian apply these product updates as well. Alternatively, Proficy HMI/SCADA customers may uninstall the Proficy Historian software if it is not in use.

Solutions

Historian installations

The following product updates address this issue:

- Proficy Historian 4.5 SIM 5 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3782
- Proficy Historian 4.0 SIM 17 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3778
- Proficy Historian 3.5 SIM 18 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3779
- Proficy Historian 3.1 SIM IH31_11420452871: http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3788

Note: Proficy SIMs are cumulative. All future SIMs will include these updates.

iFIX and CIMPLICITY installations

Option 1: Apply a product update to the Proficy Historian software.

Refer to the information above for “Historian Installations” and apply the appropriate product update to Proficy Historian.

Option 2: Uninstall Proficy Historian if not in use.

1. Double-click the Add/Remove Programs icon in the Control Panel. The Add/Remove Programs dialog box opens.
2. Select Proficy Historian, and click the Remove button.
    a. To uninstall Historian and save the current Historian configuration and data, select Do Not Delete Archives and click Next.
    b. To uninstall Historian and delete the current Historian configuration and data, select Delete Archives and click Next.
3. The uninstall proceeds and all Historian components are removed.

Vulnerability information

A memory corruption vulnerability exists in the way that the Historian Data Archiver service (ihDataArchiver.exe or ihDataArchiver_x64.exe) processes incoming TCP/IP message traffic on TCP port 14000.

Affected software

- Proficy Historian: Versions 4.5 and prior
- Proficy HMI/SCADA – CIMPLICITY: Version 8.2 (with Proficy Historian 4.5 or prior installed)
- Proficy HMI/SCADA – iFIX: Versions 5.5, 5.0 and 5.1 (with Proficy Historian 4.5 or prior installed)

Note: Proficy Pulse is not affected by the vulnerability described in this advisory.

Acknowledgements

GE Intelligent Platforms would like to thank Luigi Auriemma and the Zero Day Initiative for reporting this issue.

Change log

Date	Change(s)
February 1, 2012	• Removed an incorrect link to Historian 3.1 SIM download page
February 2, 2012	• Added the correct link to Historian 3.1 SIM download page (DN3788)
March 12, 2012	• Added CVE and ICS-CERT identifiers