ICS-CERT ADVISORY

ICSA-11-243-03**A**—GE INTELLIGENT PLATFORMS PROFICY HISTORIAN DATA ARCHIVER BUFFER OVERFLOW VULNERABILITY

UPDATE A

November 29, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-243-03P on the US-CERT secure portal on August 31, 2011. This Updated Advisory is a follow-up to the web page Advisory titled "ICSA-11-243-03—GE Intelligent Platforms Proficy Historian Data Archiver" that was published on November 01, 2011, on the ICS-CERT web page.

ICS-CERT received a report from GE Intelligent Platforms and the Zero Day Initiative (ZDI) concerning a stack-based buffer overflow vulnerability in the GE Intelligent Platforms Proficy Historian Data Archiver.

--------- Begin Update A Part 1 of 1 --------

This vulnerability was reported to ZDI by independent security researcher Luigi Auriemma.

--------- End Update A Part 1 of 1 ----------

ICS-CERT has coordinated with GE Intelligent Platforms to validate this vulnerability, and GE Intelligent Platforms has created a patch to address the issue. ICS-CERT has verified that the patch fully resolves this issue.

AFFECTED PRODUCTS

This vulnerability affects the following GE Intelligent Platforms products:

- Proficy Historian: Versions 4.0 and prior
- Proficy HMI/SCADA—CIMPLICITY: Version 8.1 (If Historian is installed)
- Proficy HMI/SCADA—iFix: Versions 5.0 and 5.1 (If Historian is installed).

IMPACT

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

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Proficy Historian is a data historian that collects, archives, and distributes production information. According to GE, the Proficy Historian product is deployed across multiple industries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

MITRE[a] has assigned number CVE-2011-1918 to this vulnerability.

A stack-based buffer overflow vulnerability exists as a result of the way that the Historian Data Archiver service (ihDataArchiver.exe or ihDataArchiver_x64.exe) processes incoming TCP/IP message traffic on Port 14000/TCP.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No publicly available exploits specifically targeting this vulnerability are known to exist.

DIFFICULTY

Exploiting this vulnerability requires a moderate skill set.

a. http://cve.mitre.org/cve/, website last accessed August 31, 2011.

MITIGATION

GE Intelligent Platforms has released security advisories and free product updates Software Improvement Modules (SIMS) to address recently reported security vulnerabilities in Proficy software. GE Intelligent Platforms urges all customers to follow the recommendations in the security advisories, which can be found at http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB14493. A valid GE SSO ID and Customer Service Number are required to access the advisories and updates.

The following product updates for Proficy Historian address this issue:

- Proficy Historian 4.0 SIM 12 at: http://support.ge-ip.com/support/index?page=dwchannel&id=DN3706
- Proficy Historian 3.5 SIM 17 at: http://support.ge-ip.com/support/index?page=dwchannel&id=DN3696
- Proficy Historian 3.1 SIM IH31_11092015699.exe at: http://support.ge-ip.com/support/index?page=dwchannel&id=DN3698

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

GE Intelligent Platforms has provided the following instructions for iFix and CIMPLICITY users:

iFIX and CIMPLICITY installations:

Option 1: If Proficy Historian is in use, refer to the information above for Historian SIM applications and apply the appropriate SIM (update) to the installed version of Proficy Historian.

Option 2: If Proficy Historian is not in use, uninstall Proficy Historian by following the instructions below:

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.

In addition to applying the patch or uninstalling, ICS-CERT recommends that customers using the affected product should consider taking the following proactive measures to decrease the likelihood of successful exploitation of this vulnerability.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

- Locate control system networks and remote devices behind firewalls with properly configured rules addressing Port 14000/TCP and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) provides a recommended practices section for control system security on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[b] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public websites. All comments or questions related to this document should be directed to the ICS-CERT at ics-cert@dhs.gov.

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed August 24, 2011.