ICS-CERT ADVISORY

ICSA-12-032-01— GE INTELLIGENT PLATFORMS PROFICY HISTORIAN DATA ARCHIVER MEMORY CORRUPTION VULNERABILITY

March 13, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-12-032-01P on the US-CERT secure portal on March 02, 2012. This web page release was delayed to allow users time to download and install the update.

ICS-CERT received a report from GE Intelligent Platforms and the Zero Day Initiative (ZDI)[a] concerning a memory corruption vulnerability in the GE Intelligent Platforms Proficy Historian Data Archiver. This vulnerability was reported to ZDI by independent security researcher Luigi Auriemma.

If exploited, this vulnerability could allow an attacker to cause the Historian Data Archiver service to crash, which may lead to arbitrary code execution.

GE Intelligent Platforms has created a patch to address the issue.

AFFECTED PRODUCTS

This vulnerability affects the following GE Intelligent Platforms products:

- 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.

IMPACT

Exploitation of this vulnerability 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.

a. http://www.zerodayinitiative.com/, website last accessed February 01, 2012

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

A memory corruption vulnerability[b] exists because of the way the Historian Data Archiver service (ihDataArchiver.exe or ihDataArchiver_x64.exe) processes incoming traffic on Port 14000/TCP. A specially crafted packet may cause the Historian Data Archiver service to crash and may allow arbitrary code execution.

CVE-2012-0229[c] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a moderate skill level would be able to exploit these vulnerabilities.

MITIGATION

GE Intelligent Platforms has released a security advisory and free product update Software Improvement Modules (SIMs) to address this vulnerability in Proficy software. GE Intelligent Platforms urges all customers to follow the recommendations in their security advisory, which can be found here: http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB14767.

Note: A valid GE user ID and Customer Service Number are required to access the advisory and update.

b. http://cwe.mitre.org/data/definitions/119.html, website last accessed March 12, 2012

c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0229, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

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.

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

GE has provided the following installation instructions for iFIX and CIMPLICITY SIMs.

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.

In addition to installing the product updates available from GE, ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- 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) also provides a section for control systems security recommended practices 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.[d] 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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[e] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[f] for more information on social engineering attacks.

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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed March 12, 2012.
e. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed March 12, 2012
f. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 12, 2012