ICS-CERT ADVISORY

ICSA-12-131-02—GE INTELLIGENT PLATFORMS PROFICY HTML HELP VULNERABILITIES

June 27, 2012

OVERVIEW

Independent researcher Andrea Micalizzi has identified a command injection vulnerability in a third-party HTML help application used by some GE Intelligent Platforms Proficy products. While analyzing this report, GE identified a stack-based buffer overflow vulnerability that also existed in the same component. These vulnerabilities were coordinated through the Zero Day Initiative (ZDI).

A remote attacker could exploit these vulnerabilities.

GE Intelligent Platforms has provided a tool to remove the unnecessary ActiveX component that introduced these vulnerabilities.

AFFECTED PRODUCTS

The following GE Intelligent Platforms products are affected:

- 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.

IMPACT

By luring a user into visiting a malicious website, an attacker could exploit these vulnerabilities to execute arbitrary code on the client or place or replace files on the client.

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

BACKGROUND

According to GE, Proficy is automation and operations management software that is deployed across multiple industries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

STACK-BASED BUFFER OVERFLOW[a]

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.

CVE-2012-2515[b] has been assigned to this vulnerability.

According to the researcher, a CVSS V2 Base score of 7.5 has been assigned.

IMPROPER NEUTRALIZTION OF SPECIAL ELEMENTS[c]

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

CVE-2012-2516[d] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a medium skill would be able to exploit these vulnerabilities with the use of social engineering.

---

a. http://cwe.mitre.org/data/definitions/121.html, website last accessed May 10, 2012

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2515 , NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

c. http://cwe.mitre.org/data/definitions/77.html website last accessed May 10, 2012

d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2516 , NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

MITIGATION

GE Intelligent Platforms recommends that the KeyHelp.ocx ActiveX control be unregistered and deleted to eliminate these vulnerabilities. GE Intelligent Platforms has recommended specific control removal instructions for each of the affected products to ensure that it continues to function properly once the control is removed. Please see their instructions at the following location: http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB14863

A username and password may be required.

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, 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.*[e] 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*[f] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[g] for more information on social engineering attacks.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed May 10, 2012.
f. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed May 10, 2012.
g. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed May 10, 2012.

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.