ICS-CERT ADVISORY

ICSA-11-243-02—GE INTELLIGENT PLATFORMS PROFICY HISTORIAN WEB ADMINISTRATOR XSS

November 01, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-243-02P on the US-CERT secure Portal on August 31, 2011.

ICS-CERT has received a report from independent security researchers Billy Rios and Terry McCorkle concerning multiple cross-site scripting (XSS) vulnerabilities in the GE Intelligent Platforms Proficy Historian Web Administrator software.

ICS-CERT has coordinated this vulnerability with GE and the researchers, and GE has made recommendations to reduce the potential attack surface. The affected product, Historian Web Administrator with Proficy Historian, is considered by GE to be a legacy component; as a result, GE is not issuing a patch for this vulnerability.

AFFECTED PRODUCTS

This vulnerability affects the following products:

- Proficy Historian: All versions
- Proficy HMI/SCADA—CIMPLICITY: Version 8.1and 8.2 (If Historian is installed).
- Proficy HMI/SCADA—iFIX: Versions 5.0 and 5.1 (If Historian is installed).

IMPACT

This vulnerability could allow an attacker to obtain information and to execute arbitrary client-side scripts to support further attacks.

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

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

An XSS vulnerability exists in the Historian Web Administrator because it lacks server-side validation of query string parameter values. Attacks that exploit these vulnerabilities require that a user visit a specially crafted URL, which injects client-side scripts into the server's HTTP response to the client.

Successful exploitation of this vulnerability could allow an attacker to obtain information and to execute arbitrary client-side scripts to support further attacks.

CVE-2011-3320[a] has been assigned to this vulnerability.

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 low to moderate skill set.

MITIGATION

GE Intelligent Platforms does not recommend that customers install or use the Historian Web Administrator component with Proficy Historian. According to GE, the Historian Web Administrator is a legacy product component that should be removed from systems running the affected software to reduce the potential attack surface. According to GE, the "Administrative Website" option will be removed from the Historian Install Wizard in future versions of the Historian product.

GE recommends that customers follow these steps to remove installed copies of the Historian Web Administrator:

1. Open Windows Explorer.
2. Navigate to the Windows directory where the Historian Web Administrator is installed. By default, this is in the IIS directory C:\inetpub\wwwroot.
3. Right click on the "Historian" folder and select "Delete" to delete that folder.

a http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3320

ICS-CERT recommends that customers using the affected product consider taking the following proactive measures to decrease the likelihood of successful exploitation of this vulnerability:

- ICS-CERT encourages asset owners to 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.

GE Intelligent Platforms advises customers to follow the recommendations in the security advisory which can be found at: http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB14493. Access to the advisory requires a valid GE SSO ID and Customer Service Number.

The Control Systems Security Program (CSSP) provides a recommended practices section for control systems security on the CSSP web page. Several recommended practices are available for reading or 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.

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

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

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:

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed October 31, 2011.

c. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed October 31,2011.

d. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed October 31, 2011.

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 provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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 (ICSs) and the public at avoidable risk.