ICS-CERT ADVISORY

ICSA-11-243-01—GE INTELLIGENT PLATFORMS PROFICY PLANT APPLICATIONS BUFFER OVERFLOW

November 01, 2011

OVERVIEW

ICS CERT originally released Advisory ICSA-11-243-01P on the US-CERT secure Portal on August 31, 2011. This web page release was delayed to allow users time to download and install the update.

ICS-CERT has received a report from GE concerning a stack-based buffer overflow vulnerability in the GE Intelligent Platform Proficy Plant Applications software suite.

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

AFFECTED PRODUCTS

This vulnerability affects Proficy Plant Applications (Version 5.0 and prior).

IMPACT

This vulnerability could cause multiple Proficy services 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

According to GE, Proficy Plant Applications suite is an Operations Management software product that is deployed across multiple industries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

GE reported that a stack-based buffer overflow vulnerability exists because of the way that Proficy Plant Applications components process incoming TCP/IP message traffic. This vulnerability affects the following services:

- Proficy Server Manager (PRProficyMgr.exe) that listens on Port 12293/TCP by default

- Proficy Server Gateway (PRGateway.exe) that listens on Port 12294/TCP by default
- Proficy Remote Data Service (PRRDS.exe) that listens on Port 12299/TCP by default
- Proficy Server License Manager (PRLicenseMgr.exe) that listens on Port 12401/TCP by default.

CVE-2011-1919[a] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No publicly available exploits are known to specifically target this vulnerability.

DIFFICULTY

Exploiting this vulnerability requires a moderate skill set.

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.

ICS-CERT and GE recommend that Proficy Plant Applications users update their systems with the latest product updates, listed below:

- Proficy Plant Applications 5.0 SIM 43 at:

  http://support.ge-ip.com/support/index?page=dwchannel&id=DN3682.
- Proficy Plant Applications 4.4.1 SIM v101 at:

  http://support.ge-ip.com/support/index?page=dwchannel&id=DN3695.

Note: According to GE, Proficy SIMs are cumulative. All future SIMs will include these updates.

In addition to installing the available updates, ICS-CERT recommends that customers using the affected products 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.

a http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1919

- Locate control system networks and remote devices behind firewalls with properly configured rules—particularly Ports 12401/TCP, 12293/TCP, 12294/TCP, and 12299/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 systems 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.

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.

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