ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-032-02—MULTIPLE MEMORY CORRUPTION VULNERABILITIES IN PROFICY PLANT APPLICATIONS

March 13, 2012

OVERVIEW

ICS-CERT received a report from GE Intelligent Platforms and the Zero Day Initiative (ZDI)[a] concerning multiple memory corruption vulnerabilities in the GE Intelligent Platforms Proficy Plant Applications. These vulnerabilities were reported to ZDI by independent security researcher Luigi Auriemma.

If exploited, these vulnerabilities could allow an attacker to cause multiple Proficy services to crash, which may lead to arbitrary code execution.

GE Intelligent Platforms has created patches to address these issues.

AFFECTED PRODUCTS

The following product and versions are affected:

- Proficy Plant Applications: Versions 5.0 and prior.

IMPACT

Exploitation of these vulnerabilities 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 these vulnerabilities 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.

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

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

Proficy Plant Applications services process incoming TCP/IP traffic in a way that creates these memory corruption[b] vulnerabilities. Exploitation of these vulnerabilities may cause Proficy services to crash or allow an attacker to gain control of the system.

PRRDS.EXE MEMORY CORRUPTION

Proficy Remote Data Service (PRRDS.exe) listens on Port 12299/TCP by default.

CVE-2012-0230[c] has been assigned to this vulnerability.

PRLICENSEMGR.EXE MEMORY CORRUPTION

Proficy Server License Manager (PRLicenseMgr.exe) listens on Port 12401/TCP by default.

CVE-2012-0231[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 moderate skill level would be able to exploit these vulnerabilities.

MITIGATION

GE Intelligent Platforms recommends that customers apply product updates to supported Proficy Plant Applications Versions 5.0 and 4.4.1. Proficy Plant Applications customers using unsupported Versions 4.3.1, 4.2.3, 4.2.2, and 215.8 should contact GE Intelligent Platforms Support for assistance with obtaining and applying a patch. GE Intelligent Platforms urges all customers to follow the

[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-2012-0230, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0231, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

recommendations in their security advisory, which can be found here: http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB14766

Note: A valid GE user ID and Customer Service Number are required to access the advisories and updates. Proficy SIMs are cumulative. All future SIMs will include these updates.

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 12299/TCP and Port 12401/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.*[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:

Do not click web links or open unsolicited attachments in e-mail messages
Refer to *Recognizing and Avoiding Email Scams*[f] for more information on avoiding e-mail scams
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 March 12, 2012.

[f] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed website last accessed March 12, 2012.

[g] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed website last accessed March 12, 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.