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

ICS-CERT ADVISORY

ICSA-12-032-03—GE INTELLIGENT PLATFORMS PROFICY REAL-TIME INFORMATION PORTAL DIRECTORY TRAVERSAL

March 13, 2012

OVERVIEW

ICS-CERT received a report from GE Intelligent Platforms and the Zero Day Initiative (ZDI)[a] concerning a directory traversal vulnerability in the GE Intelligent Platforms Proficy Real-Time Information Portal. This vulnerability was reported to ZDI by independent security researcher Luigi Auriemma.

If exploited, this vulnerability could allow an attacker to create or overwrite a file on the system running Real-Time Information Portal.

GE Intelligent Platforms has created patches to address this issue.

AFFECTED PRODUCTS

According to GE Intelligent Platforms the following product and versions are affected.

Proficy Real-Time Information Portal Versions:

- 3.5
- 3.0 SP1
- 3.0
- 2.6.

Note: Proficy Real-Time Information Portal Versions 2.5 and prior are not affected by this vulnerability

IMPACT

Exploitation of this vulnerability could allow an attacker to create or overwrite a file on the system running Proficy Real-Time Information Portal.

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

According to GE, Proficy Real-Time Information Portal is a web-based data visualization and reporting tool that is deployed across multiple industries worldwide. .vulnerability Characterization

VULNERABILITY OVERVIEW

A directory traversal[b] vulnerability exists in the Remote Interface Service (rifsrvd.exe) that runs on Port 5159/TCP by default. The Remote Interface Service creates a file on the system and does not sufficiently validate two input strings that are used to create a configuration file on the server.

The vulnerability may allow a remote attacker to:

- Set the file's name and extension (to create a new file or to overwrite an existing file)
- Supply text that will be inserted into the file.

According to GE, the vulnerability does not allow the attacker to directly execute the file and does not allow the attacker to define the file's entire contents.

CVE-2012-0232[c] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a moderate skill level may 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 Real-Time Information Portal Versions 3.5 and 3.0 SP1. Proficy Real-Time Information Portal customers using Versions 3.0 and 2.6 are encouraged to upgrade to one of the versions described above and apply the appropriate product update. GE Intelligent

[b] http://cwe.mitre.org/data/definitions/22.html, website last accessed March 12, 2012

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0232, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

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:KB14768

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 5159/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:

[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.

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.