ICS-CERT ADVISORY

ICSA-13-022-01—GE PROFICY REAL-TIME INFORMATION PORTAL INFORMATION DISCLOSURE VULNERABILTIES

January 22, 2013

OVERVIEW

This advisory provides mitigation details for multiple vulnerabilities that impact the GE Intelligent Platforms Proficy Real-Time Information Portal.

General Electric (GE) has addressed two vulnerabilities in the GE Intelligent Platforms Proficy Real-Time Information Portal. Exploitation of these vulnerabilities would result in information disclosure. The vulnerabilities can be exploited remotely.

GE has produced two security advisories (GEIP12-14[a] and GEIP12-15[b]) available on the GE Intelligent Platforms support Web site to inform customers about these vulnerabilities.

AFFECTED PRODUCTS

GE Intelligent Platforms reports that the vulnerabilities affect the following versions:

- Proficy Real-Time Information Portal: All versions.

IMPACT

CVE-2013-0651 is a security misconfiguration that, if exploited, could allow an unauthenticated remote attacker to retrieve sensitive configuration information such as system usernames and passwords for Portal data sources. The security misconfiguration is a default installation setting that can be subsequently changed.

CVE-2013-0652 is an information disclosure vulnerability that, if exploited, could allow an unauthenticated remote attacker to obtain a list of usernames for users of the Portal application

a. GEIP12-14, http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15154

b. GEIP12-15, http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15155

and a limited amount of other technical information that could aid the attacker in conducting additional 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

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

INFORMATION DISCLOSURE VULNERABILITY[c]

By default, the Portal installation creates files and folders in unauthenticated locations on the IIS or Apache Web server. An attacker can exploit this misconfiguration by making an HTTP GET request on Port 80/TCP to retrieve configuration files and other sensitive information.

CVE-2013-0651[d] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).[e]

INFORMATION DISCLOSURE VULNERABILITY[f]

Proficy Real-Time Information Portal exposes methods of a vulnerable class via Java RMI. Even with Portal authentication enabled within the application, Portal unnecessarily exposes some of these methods and allows them to be called without authentication. An attacker can exploit the vulnerability by making an RMI call over Port 80/TCP to retrieve information.

c. CWE-306: Missing Authentication for Critical Function, http://cwe.mitre.org/data/definitions/306.html, Web site last accessed January 22, 2013.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0651, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N), Web site last accessed January 22, 2013.

f. CWE-200: Information Exposure, http://cwe.mitre.org/data/definitions/200.html, Web site last accessed January 22, 2013.

CVE-2013-0652[g] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).[h]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

MITIGATION

To mitigate these information disclosure vulnerabilities, GE recommends making the following configuration changes:

- Disable “Anonymous Authentication” and “Windows Authentication.”
- Require authentication for all Portal users.
- Configure an SSL certificate to encrypt Portal application traffic.

Please see GE Intelligent Platforms Product Security Advisory GEIP12-14 and GEIP12-15 for detailed instructions.

GEIP12-14 at

http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15154

GEIP12-15 at

http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15155

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

g. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0652, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
h. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N), Web site last accessed January 22, 2013.

- 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.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[i] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Targeted Cyber Intrusion Detection and Mitigation Strategies,[j] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

i. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 22, 2013.

j.Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed January 22, 2013.

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.