ICS-CERT ADVISORY

ICSA-13-022-02—GE INTELLIGENT PLATFORMS PROFICY CIMPLICITY MULTIPLE VULNERABILITIES

January 22, 2013

OVERVIEW

This advisory provides mitigation details for multiple vulnerabilities that impact GE Intelligent Platforms Proficy HMI/SCADA—CIMPLICITY.

General Electric (GE) has addressed two vulnerabilities in GE Intelligent Platforms Proficy HMI/SCADA—CIMPLICITY: a directory transversal vulnerability and improper input validation vulnerability.

GE has released two security advisories (GEIP12-13 and GEIP12-19) available on the GE Intelligent Platforms support Web site to inform customers about these vulnerabilities.

A remote attacker could exploit these vulnerabilities.

AFFECTED PRODUCTS

The following GE Intelligent Platforms products are affected:

- Proficy HMI/SCADA – CIMPLICITY: Version 4.01 and greater, and
- Proficy Process Systems with CIMPLICITY.

IMPACT

If the vulnerabilities are exploited, they could allow an unauthenticated remote attacker to cause the CIMPLICITY built-in Web server to crash or to run arbitrary commands on a server running the affected software, or could potentially allow an attacker to take control of the CIMPLICITY server.

An attacker can exploit the vulnerabilities by sending specially crafted HTTP requests to the listening service. The attacks do not require authentication and can be conducted remotely. The vulnerable components are not enabled by default.

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 HMI/SCADA–CIMPLICITY is a Client/Server-based human-machine interface/supervisory control and data acquisition (HMI/SCADA) application, which is deployed across multiple industries.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DIRECTORY TRAVERSAL[a]

A CIMPLICITY WebView CimWeb component (substitute.bcl) does not accurately check input variables. By sending a maliciously crafted packet to Port 80/TCP, an attacker could cause a directory traversal and view or download files from the server. The vulnerable component is installed by default but is enabled only when Web-based access to CIMPLICITY is in use.

CVE-2013-0653[b] has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:N/A:N).[c]

IMPROPER INPUT VALIDATION[d]

The CimWebServer does not properly validate inputted information. By sending a specially crafted packet, an attacker could crash the built-in Web server, run arbitrary commands on a server running the affected software, or take control of the server. The vulnerable CIMPLICITY built-in Web server component is not enabled by default.

[a] CWE, http://cwe.mitre.org/data/definitions/22.html, CWE-22: Path Transversal, Web site last accessed January 22, 2013.

[b] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0653 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

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

[d] CWE, http://cwe.mitre.org/data/definitions/20.html, CWE-20: Improper Input Validation, Web site last accessed January 22, 2013.

CVE-2013-0654[e] has been assigned to this vulnerability. A CVSS v2 base score of 8.8 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:C/A:C).[f]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

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

GE has created patches and has detailed configuration recommendations to mitigate these vulnerabilities:

- GEIP12-13 at http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15153
- GEIP12-19 at http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15244

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, 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.

[e] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0654 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[f] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:C/A:C), Web site last visited January 16, 2013.

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.[g] 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,[h] 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.

Previous recommendations can be used as needed. List other products that are specific to the topic (i.e., phishing mitigations):

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 email messages.
2. Refer to Recognizing and Avoiding Email Scams[i] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[j] for more information on social engineering attacks.

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

[h] 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.

[i] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed January 22, 2013.

[j] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed January 22, 2013.

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/.

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.