



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

# ICS-CERT ADVISORY

## ICSA-12-341-01—GE PROFICY HMI/SCADA CIMPLICITY INTEGER OVERFLOW

January 8, 2013

### OVERVIEW

This updated advisory is a follow-up to the original ICS-CERT Advisory titled ICSA-12-341-01P—GE PROFICY HMI/SCADA CIMPLICITY INTEGER OVERFLOW that was published December 06, 2012, to the US-CERT secure Portal library.

Researcher Kuang-Chun Hung of Information and Communication Security Technology Center (ICST) has identified an improper input validation vulnerability in GE's Intelligent Platforms Proficy HMI/SCADA—Cimplicity. This vulnerability could lead to a possible denial of service (DoS).

GE has produced an updated product version that ICST has validated. ICST confirms that the product update resolves the reported vulnerability.

This vulnerability can be exploited remotely.

### AFFECTED PRODUCTS

The following products and versions are affected:

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

Note: Proficy HMI/SCADA—CIMPLICITY Versions 4.0 and prior are not affected by this vulnerability.

This product is provided subject only to the Notification Section as indicated here: <http://www.us-cert.gov/privacy/>



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

### IMPACT

If exploited, this vulnerability could allow an unauthenticated remote attacker to cause the CIMPLICITY built-in Web server to crash or to stop responding to requests.

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

## VULNERABILITY CHARACTERIZATION

### VULNERABILITY OVERVIEW IMPROPER INPUT VALIDATION VULNERABILITY<sup>a</sup>

A vulnerability exists in the way that the CIMPLICITY built-in Web server (CimWebServer.exe) processes incoming HTTP traffic because of insufficient input validation. The CIMPLICITY built-in Web server is not enabled by default. When enabled, it listens on Port 80 TCP by default.

An attacker can exploit the vulnerability by sending malformed HTTP requests to the listening service. The attack does not require authentication and can be conducted remotely.

CVE-2012-4689<sup>b</sup> has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N/A:C).<sup>c</sup>

### VULNERABILITY DETAILS

#### EXPLOITABILITY

This vulnerability could be exploited remotely.

a. CWE-20: Improper Input Validation <http://cwe.mitre.org/data/definitions/20.html>, Web site last accessed January 08, 2013.

b. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4689>, 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=\(AV:N/AC:M/Au:N/C:N/I:N/A:C\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:N/A:C)) Web site last visited January 08, 2013.



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

### EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

### DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

### MITIGATION

GE has released a security advisory and patches to address this issue:

<http://support.ge-ip.com/support/index?page=kbchannel&id=S:KB15153>

Patches for versions of CIMPLICITY prior to Version 8.0 will not be created. GE recommends customers who are unable to patch or upgrade consider the recommendations below.

GE has provided the following workaround recommendations that eliminate the need to use the vulnerable component:

#### **Option 1: Disable the CIMPLICITY built-in Web server if it is not in use.**

GlobalView, WebView, and ThinView expose the existing functionality of the CIMPLICITY HMI application so that it can be viewed via a Web browser.

If this functionality is not required, Web-based access can be disabled by the following process:

1. Open CIMPLICITY Options.
2. Select the “WebView/ThinView” tab.
  - a. Uncheck the “Use built-in Web server” option.
  - b. Uncheck the “Start at boot time” option.
3. Select the “GlobalView” tab (if GlobalView is installed).
  - a. Uncheck the “Use built-in Web server” option.
  - b. Uncheck the “Start at boot time” option.
4. Click “OK.”

#### **Option 2: Use an alternate Web server to host GlobalView, WebView, or ThinView.**

The CIMPLICITY built-in Web server can be replaced with a third-party Web application server such as Microsoft IIS.

To configure GlobalView, WebView, or ThinView to use IIS:



## ICS-CERT

### INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

---

1. Clear the “Use built-in Web server” check box on the WebView/ThinView and GlobalView tabs of the CIMPLICITY Options dialog box.
2. Copy the ProwlerClient.jar file from the WebPages directory of your CIMPLICITY installation to an IIS Web server directory.
3. In the WebView/ThinView or GlobalView tab of CIMPLICITY Options, click on “Create a Web Page” to create an HTML file for your Web server. Use the “Browse Page” button to navigate to the directory where you’d like to save the page.

**Important:** If you would like to publish the Web page to Microsoft IIS, make sure you save the Web page to an IIS Web directory. By default, this is C:\InetPub\wwwroot or a subdirectory, but it could be another location depending on your IIS configuration. You can save the page by clicking the “Browse Page” button and navigating to the directory or by saving the file to another location and copying it to an IIS directory later.

The vulnerable service (CimWebServer.exe) will still run on the system in the “Option 2” configuration. However, because it is no longer listening on a port that is processing HTTP traffic, the vulnerability is not exposed.

As with any third-party product, ensure that your IIS Web server is up to date with the latest security patches and follow any secure configuration recommendations from the vendor.

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.

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

---

d. CSSP Recommended Practices, [http://www.us-cert.gov/control\\_systems/practices/Recommended\\_Practices.html](http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html), Web site last accessed January 08, 2013.



## ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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 Strategy,<sup>e</sup> that is available for download from the ICS-CERT Web page ([www.ics-cert.org](http://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](mailto:ics-cert@hq.dhs.gov)

Toll Free: 1-877-776-7585

For industrial control systems security information and incident reporting: [www.ics-cert.org](http://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.

**May I edit this document to include additional information?** This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public Web sites. All comments or questions related to this document should be directed to ICS-CERT at [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).

**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

---

e. Targeted Cyber Intrusion Detection and Mitigation Strategies, [http://www.us-cert.gov/control\\_systems/pdf/ICS-TIP-12-146-01A.pdf](http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf), Web site last accessed January 08, 2013.



## **ICS-CERT**

**INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM**

---

development of proper mitigations may put industrial control systems and the public at avoidable risk.