GE Intelligent Platforms Product Security Advisory

Title: Multiple vulnerabilities in Proficy HMI/SCADA – CIMPLICITY built-in Web server
Vulnerability ID: GEIP12-13
Other identifiers: KB15153
Release date: October 2, 2012
Last updated: December 3, 2012

Summary

Vulnerabilities have been identified in Proficy HMI/SCADA – CIMPLICITY that, if exploited, 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. The command execution vulnerability could potentially allow an attacker to take control of the CIMPLICITY server. The vulnerable CIMPLICITY built-in Web server component is not enabled by default.

GE Intelligent Platforms is aware of exploits that exist for these vulnerabilities. However, as of the latest update to this advisory, we are not aware of any reports of the vulnerabilities being exploited in customer environments.

GE Intelligent Platforms recommends that customers apply product updates to Proficy HMI/SCADA – CIMPLICITY's supported versions 8.2, 8.1, and 8.0.

Proficy HMI/SCADA – CIMPLICITY customers using versions prior to 8.0 are encouraged to consider the alternatives and recommendations outlined in the "Workarounds" section of this document or to upgrade to one of the versions described above and apply the appropriate product update.

Affected software

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

Note: Proficy HMI/SCADA – CIMPLICITY versions 4.0 and prior are not affected by this vulnerability

Solution

The following product updates address this issue:

- Proficy HMI/SCADA – CIMPLICITY 8.2 SIM 12 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3911
- Proficy HMI/SCADA – CIMPLICITY 8.1 SIM 19 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3910
- Proficy HMI/SCADA – CIMPLICITY 8.0 SIM 24 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3913

Note: Proficy SIMs are cumulative. All future SIMs will include these updates.

SIMs for versions of CIMPLICITY prior to version 8.0 will not be created. Customers using these older versions of the software should consider the alternatives outlined in the "Workarounds" section of this document or consider upgrading to a supported version of the product.

Workarounds

The following workarounds 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:

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 webserver. 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 sub-directory, 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.

Note that the vulnerable service (CimWebServer.exe) will still run on the system in the "Option 2" configuration but because it is no longer listening on a port and 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.

Vulnerability information

Multiple vulnerabilities exist in the way that the CIMPLICITY built-in Web server (CimWebServer.exe) processes incoming HTTP traffic, both due to a lack of sufficient input validation. The vulnerable CIMPLICITY built-in web server is not enabled by default. When enabled, it listens on port 80 by default.

An attacker can exploit the vulnerabilities by sending malformed HTTP requests to the listening service. The attacks do not require authentication and can be conducted remotely.

Acknowledgement

GE Intelligent Platforms would like to thank Kuang-Chun Hung of Information and Communication Security Technology Center (ICST) for reporting a denial of service issue covered in this advisory via ICS-CERT and for helping to protect our customers.

Disclaimer

Change log

Date	Change(s)
October 2, 2012	• Initial release
November 13, 2012	• Added links to SIMs • Added additional info about behavior of CimWebServer.exe with workaround "Option 2"
December 3, 2012	• Added acknowledgement for DoS issue