GE Intelligent Platforms Product Security Advisory

Title: Remote code execution in Proficy HMI/SCADA – CIMPLICITY WebView
Vulnerability ID: GEIP13-06
Other identifiers: KB15940, ZDI-CAN-1623
Release date: December 19, 2013
Last updated: December 18, 2013

Summary

A vulnerability has been identified in **Proficy HMI/SCADA – CIMPLICITY WebView** that, if exploited, could allow an unauthenticated remote attacker to execute arbitrary commands on a server running the affected software. This command execution vulnerability could potentially allow an attacker to take control of the CIMPLICITY server. The vulnerable CIMPLICITY WebView component is not enabled by default.

GE Intelligent Platforms recommends that customers apply product updates to Proficy HMI/SCADA – CIMPLICITY version 8.2.

Proficy HMI/SCADA – CIMPLICITY customers using versions prior to 8.2 are encouraged to consider the alternatives and recommendations outlined in the "Other Recommendations" section of this document or to upgrade to version 8.2 and apply the appropriate product update.

GE Intelligent Platforms has been notified that this vulnerability may be publically disclosed as early as December 31, 2013. Customers are strongly urged to follow the instructions in this document as soon as possible.

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 update addresses this issue:

- Proficy HMI/SCADA – CIMPLICITY 8.2 SIM 24 at http://support.ge-ip.com/support/index?page=dwchannel&id=DN4128

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

SIMs for versions of CIMPLICITY prior to version 8.2 will not be created. Customers using these older versions of the software should consider the alternatives outlined in the "Other Recommendations" section of this document or consider upgrading to a supported version of the product.

Instructions

Step 1: Apply the latest Product Update to the affected software.

Step 2: If the production configuration includes CimView screens that are located on remote servers, access to those screens will be denied until additional configuration is provided. To enable access to CimView screens located on a remote server, add the UNC paths for the required remote directories to the Directory Whitelist in the CIMPLICITY Options. See the CIMPLICITY online help for detailed instructions.

Note: As with any configuration change, you should perform testing to ensure acceptable operation prior to deploying changes in a production environment.

Other Recommendations

The following recommendations may eliminate or mitigate the impact of the vulnerability.

Disable CIMPLICITY's web-based HMI functionality 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"

Disable WebView and instead use GlobalView with IIS to access CIMPLICITY screens via a web browser

The vulnerable "CimWebServer.exe" will not run if GlobalView is configured to run with the IIS web server. However, you must be sure to *disable the CIMPLICITY built-in web server with GlobalView* as follows:

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
4. Click "OK"

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

A vulnerability exists in the way that the CIMPLICITY WebView component (CimWebServer.exe) processes incoming requests over TCP port 10212, due to a lack of sufficient input validation. The vulnerable CIMPLICITY WebView component is not enabled by default.

This vulnerability can be exploited remotely and without authentication by sending a malicious message over a TCP connection to the listening service.

Acknowledgements

GE Intelligent Platforms would like to thank security researchers ZombiE and amisto0x07 for reporting this issue via HP TippingPoint's Zero Day Initiative and for helping to protect GE customers.

Disclaimer

Change log

Date	Change(s)
December 19, 2013	• Initial release