GE Intelligent Platforms Product Security Advisory

Title: Multiple vulnerabilities in Proficy HMI/SCADA – CIMPLICITY WebView
Vulnerability ID: GEIP13-03
Other identifiers: KB15602, ZDI-CAN-1621, ZDI-CAN-1624
Release date: June 18, 2013
Last updated: June 17, 2013

Summary

Multiple vulnerabilities have been identified in Proficy HMI/SCADA – CIMPLICITY WebView that, if exploited, could allow an unauthenticated remote attacker 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 WebView component is not enabled by default.

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 "Other Recommendations" 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 to 8.2
- 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 these issues:

- Proficy HMI/SCADA – CIMPLICITY 8.2 SIM 19 at http://support.ge-ip.com/support/index?page=dwchannel&id=DN4014
- Proficy HMI/SCADA – CIMPLICITY 8.1 SIM 25 at http://support.ge-ip.com/support/index?page=dwchannel&id=DN4024
- Proficy HMI/SCADA – CIMPLICITY 8.0 SIM 27 at http://support.ge-ip.com/support/index?page=dwchannel&id=DN4013

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 "Other Recommendations" section of this document or consider upgrading to a supported version of the product.

Other Recommendations

The following recommendation 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

Multiple vulnerabilities exist 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.

An attacker can exploit the vulnerabilities by sending malicious message over TCP connection to listening service. The attacks do not require authentication and can be conducted remotely.

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)
June 18, 2013	• Initial release