GE Intelligent Platforms Product Security Advisory

Title: Proficy HMI/SCADA – CIMPLICITY Targeted by an Advanced Threat Actor
Vulnerability ID: GEIP14-05
Other identifiers: KB16399, CVE 2014-0751
Release date: October 28, 2014
Last updated: October 27, 2014

Summary

GE Intelligent Platforms has become aware of an ongoing targeted campaign by an Advanced Persistent Threat - see CVE-2014-0751.

- Among the attack vectors, adversaries may leverage outdated Proficy HMI/SCADA – CIMPLICITY servers routable through the public internet or business network.
- Adversaries may engage in a phishing campaign by attaching malicious CimView Screen (.CIM, .CTX, .CIMRT) files.

GE Intelligent Platforms recommends that customers upgrade to Proficy HMI/SCADA – CIMPLICITY 8.2 SIM 24 or later, enable additional security controls and exercise caution when working with CimView files received from unknown sources.

Proficy HMI/SCADA – CIMPLICITY customers unable to upgrade to version 8.2 are encouraged to consider the alternatives and recommendations outlined in the "Other Recommendations" section of this document.

Affected software

Proficy HMI/SCADA – CIMPLICITY: Version 8.2 with SIM 23 and prior

Solution

Beginning with CIMPLICITY v8.2 SIM 24, a Whitelist feature that is only used by WebView is included in the CIMPLICITY Options dialog box. If the WebView server is not required to open files on remote shares there is no other configuration required. If the WebView server does require access to remote shares they will need to be added to the whitelist. The whitelist only impacts CimView in a WebView session.

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

Note: Proficy SIMs are cumulative. All future SIMs will include these updates. The SIM listed above may be replaced with newer ones in the future. The latest SIMs are always available for download at http://support.ge-ip.com.

Other Recommendations

Patches and Security Updates:

- Please make sure your installation of CIMPLICITY has all the latest updates installed. The latest SIMs are always available for download at http://support.ge-ip.com.
- Follow GE Intelligent Platforms Security Advisories (KB14607) to address all known vulnerabilities that apply to your environment - especially GEIP13-05 and GEIP13-06 as those are suspected to be leveraged in this campaign.

Exposure to Public Networks:

- Avoid exposure of your control environment and CIMPLICITY servers to the public internet and business network.
- Prevent outgoing requests to unknown file shares located outside your control environment.

Beware of Malicious CimView (.CIM, .CTX, .CIMRT) Files:

- Avoid using .CIM, .CTX, and .CIMRT (CimView) files received from unknown sources.
- Avoid sending unprotected CimView files over unencrypted networks or public internet.
- Consider using a strong hashing algorithm to validate the integrity of created CimView files and ensure they haven't been tampered with over time.

Monitor Your Control Network for Suspicious Activity:

- Examine CIMPLICITY WebView connections log(s). These are typically located in C:\Program Files (x86)\Proficy\Proficy CIMPLICITY\log\WebThin_Connections_*N*.csv, where *N* will be a number, and 1 will indicate the most recent log file. Look for signs of suspicious activity such as unfamiliar network paths and unfamiliar file names.
- Follow best practices on securing Industrial Control Systems and applicable technology stacks.
- Consider additional intrusion detection and prevention countermeasures.
- US ICS-CERT strongly encourages control system operators to be aware of the signs of compromise and immediately report to ICS-CERT for further analysis and correlation.

Vulnerability information

A group of adversaries named "Sandworm" is implementing a targeted campaign against select targets in the United States and abroad. Among the attack vectors, adversaries may engage in phishing campaigns, leverage known and 0-day vulnerabilities and target vulnerable ICS, SCADA and HMI systems routable through public networks.

Disclaimer

Product advisories provided here are subject to terms and conditions contained in customers' underlying license agreements or other applicable agreements. Due to ongoing product enhancements, GE reserves the right to change or update advisories without advance notification.

Change log

Date	Change(s)
10/28/2014	• Initial release