GE Intelligent Platforms Product Security Advisory

Title: Proficy HMI/SCADA – CIMPLICITY CimView Memory Access Violation
Vulnerability ID: GEIP14-02
Other identifiers: KB16331, ICS-VU-632700, CVE-2014-2355
Release date: September 19, 2014
Last updated: August 29, 2014

Summary

A vulnerability has been identified in Proficy HMI/SCADA – CIMPLICITY CimView that, if exploited, could allow an attacker to execute arbitrary commands on a computer running the affected software.

GE Intelligent Platforms recommends that customers apply product updates to Proficy HMI/SCADA – CIMPLICITY version 8.1 and 8.2. If you are using a version of CIMPLICITY prior to version 8.1, please contact your local GE Intelligent Platforms representative for upgrade options. Contact information is also available at http://www.ge-ip.com/contact.

In cases where upgrade is not feasible customers using CIMPLICITY versions prior to 8.1 are advised to consider the alternative recommendations outlined in the "Other Recommendations" section of this document.

Affected software

Proficy HMI/SCADA – CIMPLICITY: Version 8.2 and prior

Solution

The following product updates addresses this issue:

- Proficy HMI/SCADA – CIMPLICITY 8.2 SIM 26 (DN4197)
  http://support.ge-ip.com/support/index?page=dwchannel&id=DN4197
- Proficy HMI/SCADA – CIMPLICITY 8.1 SIM 29 (DN4219)
  http://support.ge-ip.com/support/index?page=dwchannel&id=DN4219

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

For customers using a version of CIMPLICITY prior to version 8.1 and unable to upgrade, the following recommendations may eliminate or mitigate the impact of the vulnerability:

- Take steps to properly secure and protect stored Cimplicity Screen files (.CIM).
- Avoid using .CIM files received from unknown sources.

- Avoid sending unprotected .CIM files over unencrypted networks or public internet.
- Consider using strong hashing algorithm to validate integrity of created .CIM files and ensure they haven't been tampered with over time.

Vulnerability information

A vulnerability exists in the way that the CIMPLICITY CimView and CIMPLICITY CimEdit components process information stored in CIMPLICITY screen (.CIM) files. A specially crafted .CIM file could potentially lead to a memory access violation and/or arbitrary code execution.

Acknowledgements

GE Intelligent Platforms would like to thank Said Arfi for reporting this issue via ICS-CERT and for helping to protect our customers.

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)
9/19/14	• Initial release