GE Intelligent Platforms Product Security Advisory

Title: Multiple memory corruption vulnerabilities in Proficy Plant Applications
Vulnerability ID: GEIP12-02
Other identifiers: KB14766, CVE-2012-0230, CVE-2012-0231, ICS-VU-426246, ZDI-CAN-1377
Release date: January 31, 2012
Last updated: March 12, 2012

Summary

A vulnerability exists in Proficy Plant Applications that, if exploited, could potentially allow an attacker to cause multiple Proficy services to crash or take control of a system running the affected software.

GE Intelligent Platforms recommends that customers apply product updates to supported Proficy Plant Applications versions 5.0 and 4.4.1. Proficy Plant Applications customers using unsupported versions 4.3.1, 4.2.3, 4.2.2, and 215.8 should contact GE Intelligent Platforms Support for assistance with obtaining and applying a patch.

Customers using other versions are encouraged to upgrade to one of the supported versions described above and apply the appropriate product update.

Solutions

The following product updates address this issue in supported versions:

- Proficy Plant Applications 5.0 SIM 62 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3783
- Proficy Plant Applications 4.4.1 SIM 106 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3784

Patches have also been developed for Proficy Plant Applications versions 4.3.1, 4.2.3, 4.2.2, and 215.8. Customers using these versions should contact GE Intelligent Platforms Support for assistance with obtaining and applying the patch.

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

Vulnerability information

Memory corruption vulnerabilities exist in the way that the following Proficy Plant Applications services process incoming TCP/IP message traffic:

- Proficy Remote Data Service (PRRDS.exe) that listens on TCP port 12299 by default
- Proficy Server License Manager (PRLicenseMgr.exe) that listens on TCP port 12401 by default

Affected software

- Proficy Plant Applications: Versions 5.0 and prior

Acknowledgements

GE Intelligent Platforms would like to thank Luigi Auriemma and the Zero Day Initiative for reporting this issue.

Change log

Date	Change(s)
March 12, 2012	• Added CVE and ICS-CERT identifiers • Updated status of patches for unsupported versions in Solution section