GE Intelligent Platforms Product Security Advisory

Title: Proficy Portal directory traversal
Vulnerability ID: GEIP12-03
Other identifiers: KB14768, CVE-2012-0232, ICS-VU-481091, ZDI-CAN-1419
Release date: January 31, 2012
Last updated: March 12, 2012

Summary

A vulnerability exists in Proficy Real-Time Information Portal that, if exploited, could allow an attacker to create or overwrite a file on the system running Real-Time Information Portal.

GE Intelligent Platforms recommends that customers apply product updates to Proficy Real-Time Information Portal versions 3.5 and 3.0 SP1. Proficy Real-Time Information Portal customers using versions 3.0 and 2.6 are encouraged to upgrade to one of the versions described above and apply the appropriate product update.

Solutions

The following product updates address this issue:

- Proficy Real-Time Information Portal 3.5 SIM 11 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3785
- Proficy Real-Time Information Portal 3.0 SP1 SIM 42 at http://support.ge-ip.com/support/index?page=dwchannel&id=S:DN3786

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

Mitigations

The following configuration changes may mitigate the impact of a successful exploit of this vulnerability:

- Install Proficy Real-Time Information Portal on a separate hard drive partition from the operating system
- Reconfigure default Windows user accounts for security: Rename the “Administrator” account and disable the “Guest” account

Vulnerability information

A directory traversal vulnerability exists in the Remote Interface Service (rifsrvd.exe) which runs on TCP port 5159 by default. The Remote Interface Service creates a file on the system and does not sufficiently validate two input strings that are used to create a configuration file on the server.

The vulnerability allows a remote attacker to:

- Set the file's name and extension (to create a new file or to overwrite an existing file)
- Supply text that will be inserted into the file

The vulnerability does not allow the attacker to directly execute the file and does not allow the attacker to define the file's entire contents.

Affected software

- Proficy Real-Time Information Portal: Versions 3.5, 3.0 SP1, 3.0, and 2.6

  Note: Versions of Proficy Real-Time Information Portal version 2.5 and prior are not affected by this vulnerability

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