NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

CIP: GE Fanuc iFIX Vulnerability

Initial Distribution: February 10, 2009

This vulnerability was publicly announced on February 1, 2009. No known exploits currently exist.

Why am I receiving this? >>
About NERC Alerts >>

Status:	Information Only: No Reporting Required
	**Public: No Restrictions. Will be posted to NERC's Web site alert page.** **More on handling >>**
Instructions:	This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a Reliability Standard. NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.**
Distribution:	**Initial Distribution: Primary Compliance Contacts** Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Load Serving Entities, Distribution Providers **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	SCADA, EMS, Operations, Planning, IT Security. Transmission Operators, Transmission Owners, Generation Operators, Generation Owners, Load Serving Entities, Distribution Providers using GE Fanuc iFIX (all versions).
Advisory:	A vulnerability in all versions of GE Fanuc iFix has been publicly released. An attacker exploiting this vulnerability would be able to gain administrator privileges to the GE Fanuc iFIX process and manipulate data, control connected devices by manipulating the Human Machine Interface (HMI) or degrade Situational Awareness. Users of GE Fanuc iFIX are advised to: • Disable the Windows AutoPlay feature • Isolate the network where iFIX resides from less trusted networks • Require authentication to the machine (not just the HMI) • Provide physical and cyber security to limit access to network where iFIX resides • Enable Windows authentication within iFIX product • Use Windows roles and privileges and do not allow administrative access for operators of the product • Store the password file in a protected fashion making use of administrative level privileges regardless of location A detailed Knowledge Base article on the vulnerability and its mitigation is available on the GE Fanuc Support site at: http://support.gefanuc.com/support/index?page=kbchannel&id=KB13253

Advisory:
(continued from previous page)

Currently no remediation exists; and there is no released patch for the vulnerability.

Users are advised to contact GE Fanuc (phone: 1-800-GE Fanuc, e-mail: support@gefanuc.com) for further information.

The ES-ISAC estimates that the risk to bulk power system reliability from this vulnerability is LOW, due to existing security at the network level, no evidence of exploitation code being released into the public, and the relatively high level of expertise needed to modify the dynamically linked library.

Background:

Actions that can be taken by an attacker are:

1. If the recommended Windows authentication mode is not utilized, the iFIX security file can be reverse-engineered to obtain the user's password.

2. A user can bypass authentication if they have privileged administrative access to the Windows host by loading a specially modified dynamically linked library.

3. Environment protection can be bypassed by attaching an external storage that supports AutoPlay and contains an automatically launched script.

US CERT Vulnerability Note VU#310355

Contact:

Doug Newbauer
Manager of Alerts
609.937.3413
doug.newbauer@nerc.net

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
609.452.1422
esisac@nerc.com

A-2009-02-10-01