



Vendor Statement for CERT CVE-2009-0216

CERT has reported vulnerabilities in iFIX (versions PDE, 2.0, 2.2, 2.21, 2.5, 2.6, 3.0, 3.5, 4.0, 4.5, and 5.0). The vulnerabilities involve iFIX security, and can be exploited when it is used and an attacker has direct or network access to a HMI/SCADA or VIEW node. The consequence of a successful exploit is that an attacker will have elevated privilege to the HMI/SCADA node. This document describes these vulnerabilities and mitigating steps.

iFIX contains a number of features designed to authenticate operators and to enforce their associated privileges. To accomplish authentication, iFIX allows administrators to create a user name and password for each operator authorized to use the system. The user name and password are stored locally on the HMI/SCADA machine in a local file. When an operator wants to request authentication, he will start the program "Login.exe," which prompts him for his user name and password. Once authenticated, the user may modify process information depending on his privilege set.

One privilege that may be assigned or denied to operators is the ability to task switch away from the workspace. This is known as *environment protection* and can prevent the interactive user from direct access to interactive shells, preventing him from launching unauthorized programs or accessing the core operating system. The intent of this feature is to limit the operator from misusing the computer while allowing HMI/SCADA application access.

The following vulnerabilities impact the features described above:

- (1) An attacker can use a cryptographic attack to extract passwords from iFIX security files.

Username and passwords are stored in a local file. The information is stored in a binary format with the password encrypted using a simple algorithm designed to obscure passwords. This algorithm is reversible, so if an attacker is able to copy this file, he can retrieve the passwords using a reverse encryption algorithm.

Attackers can gain copies of this file in two ways. The first way requires that an attacker have an interactive session with the computer containing the file, such as a direct login, or through a remote terminal session, VNC, or some other remote session providing access to a command shell. Using the shell, the attacker can simply copy the file and extract the passwords at some later point. Another way an attacker can gain access to this file is by intercepting the file over the network. This can occur if the file is shared between two computers using Microsoft Windows® network sharing. In this case, an

attacker may be able to recreate the file by using a network sniffer to monitor network traffic between them.

(2) A user can bypass authentication by loading a specially modified software module.

Authentication and authorization of users are implemented through certain program modules. These modules can be modified at the binary level to bypass user authentication. To exploit this type of attack, an attacker needs to be able to launch unauthorized applications from an interactive shell. The binary modification requires some expertise to perform.

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

Autoplay allows for the launching of application from a CD ROM, a USB key, or some other removable storage. An attacker can create a CD or USB key with an application set up to run when the storage is inserted into the computer. Environment protection does not disable autoplay. See CERT's tech alert concerning Microsoft® autoplay (<http://www.us-cert.gov/cas/techalerts/TA09-020A.html>) for more details.

The approach to mitigating these issues is to prevent users from launching unauthorized programs or sniffing or copying of the security file. GE Fanuc recommends the following mitigations.

1. Disable the Windows autoplay feature, as described by (<http://www.us-cert.gov/cas/techalerts/TA09-020A.html>). Alternatively apply the SIM related to 1-668890121. This step will prevent users from bypassing environment protection.
2. Enable environment protection for those users should not have administrative privileges.

To use environment protection, first ensure that administrators have privileges to task switch and execute CTRL-ALT-DEL, as shown in Figure 1. Other users, who should not have access to the Windows Desktop should not have these privileges. This is configured through the System Configuration Utility (SCU).

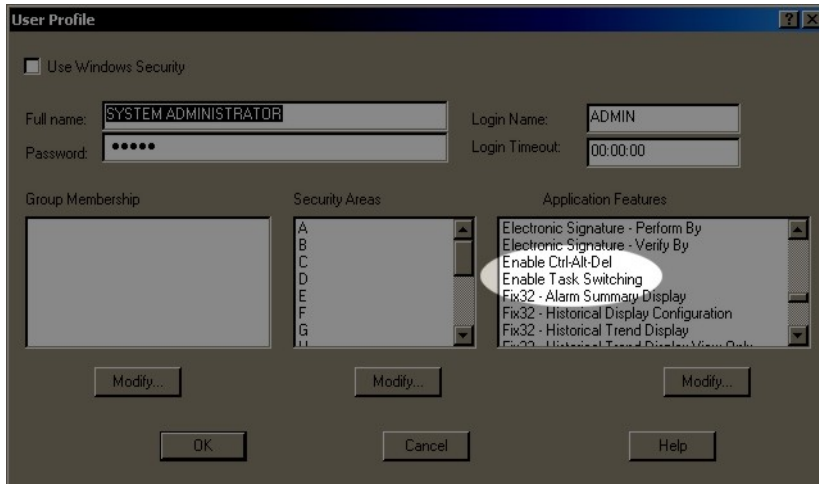


Figure 1 Rights For Administrators

Next, enable environment protection by opening the iFIX Workspace in configure mode and selecting in the menu Workspace->User preferences. Enable the environment protection, as shown in Figure 2.

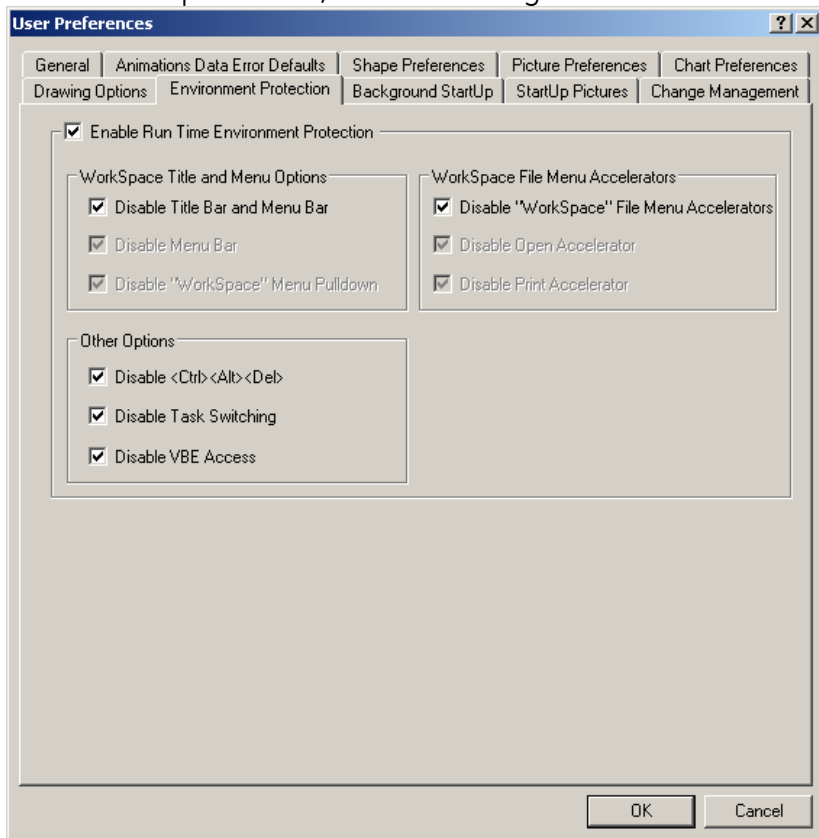


Figure 2 Enabling Environment Protection

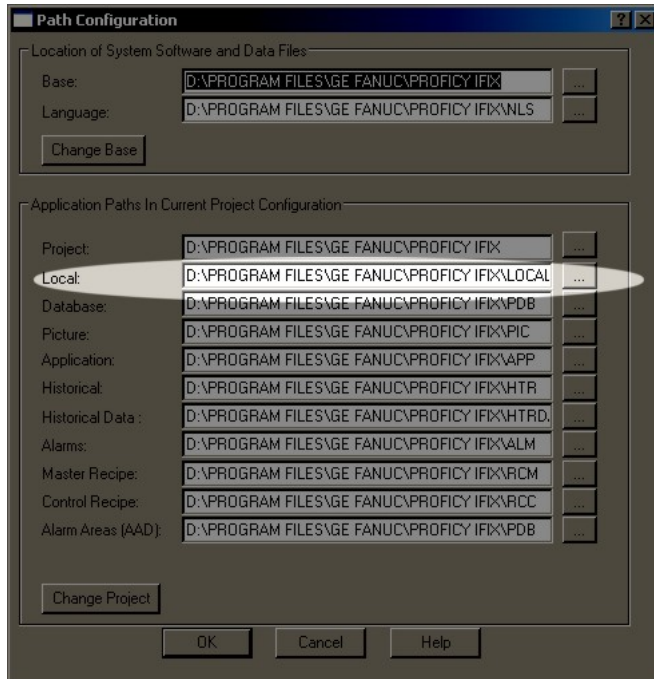


Figure 3 SCU Path Configuration

3. The security files are located in the iFIX local directory, as indicated in the SCU. Do not share the iFIX Local directory either directly or as a subdirectory of a shared directory. Ensure administrative shares are disabled.

Many end-users share the security files through Microsoft network sharing, as it makes it convenient to coordinate security changes among nodes. Using sharing in this way may expose the security file to interception if an attacker has penetrated into the HMI/SCADA sub-network.

4. Isolate the iFIX HMI/SCADA network from the corporate network using firewalls. IT administrators should be particularly watchful for intrusions into the HMI/SCADA network.

The steps above will prevent operators and attackers from exploiting these vulnerabilities. Additionally for iFIX versions 4.5 and above, GE Fanuc recommends that users enable the Trusted Computing feature. The Trusted Computing feature is enabled in the SCU network configuration dialog. Please consult the online document for details on this feature.

Other steps users should consider include

5. Computer hardware on the factory floor or in control rooms should be secured in locked cabinets. If this is not possible, secure external USB ports such that they are inaccessible to the operator. If this is impractical due to the need of the iFIX hardware key, consider obtaining a software based license key from your GE Fanuc distributor.

- Utilize Windows authentication for your users. Windows authentication utilizes the operating system to maintain authentication information, such as the user name and password. This feature is enabled on a per user basis within the SCU security configurator.

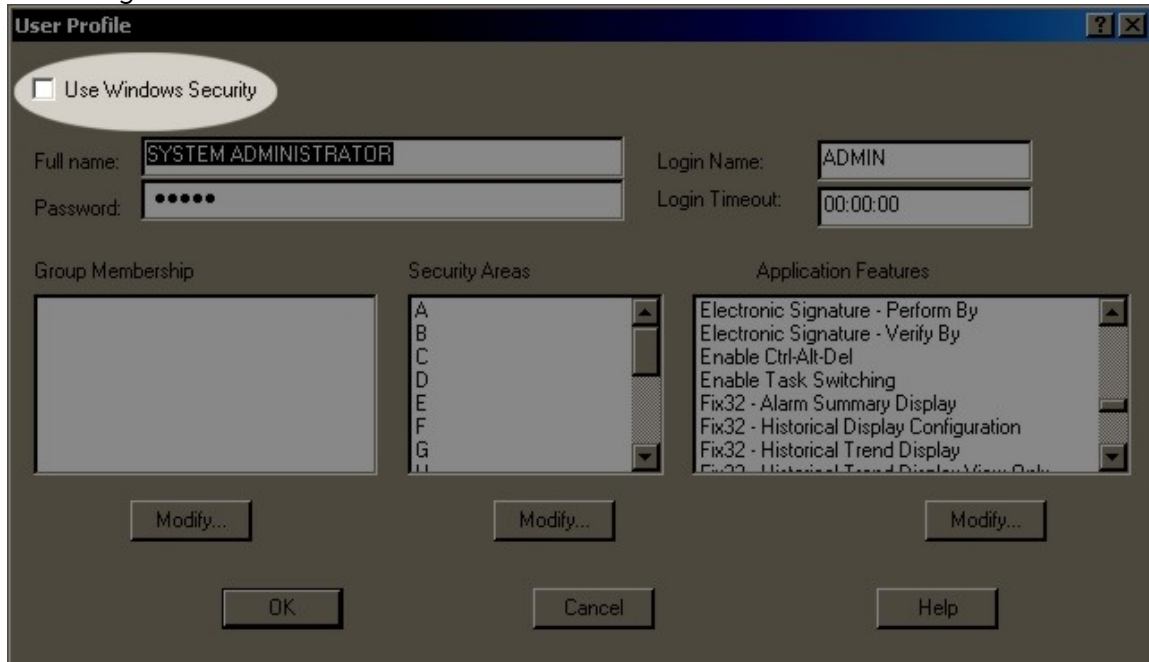


Figure 4 Enabling Windows Authentication

- Consider operating iFIX such that the operators use only View nodes to view process information instead of directly using HMI/SCADA nodes. While this does not directly deal with the issues here, it removes operators from direct regular access to the HMI/SCADA node itself.

GE Fanuc treats computing security as a very serious matter. As we identify vulnerabilities in our software, we will address them as product support issues and release as SIMS. In addition, through our customer support site, we can fast track those issues that identify a hacking vulnerability.

We need to remember that those who are interesting in hacking HMI/SCADA software are dedicated in their craft. New ways of hacking software are constantly discovered. The most important actions are to deploy security-based policies, processes and systems into existing systems and update the new system specs. It is important that customers protect their HMI/SCADA assets behind firewalls, just as they would protect the physical HMI/SCADA hardware in locked cabinets. This is the safest method of protecting HMI/SCADA systems against unknown attack vectors.