GE FANUC CIMPLICITY HMI US-CERT VULNERABILITY

Date: December 1, 2017

Overview:

Certain versions of the software supporting HMI Cimplicity systems are vulnerable to heap buffer overflow. This vulnerability may be exploited through a specially crafted packet distributed over the network.

Environment:

Older versions of HMI Cimplicity and Windows (NT and XP)

Mark* V VI VIe Ve control systems

Resolution:

The risk of attack by an external/internal hacker depends on site-specific network configurations. Every site is encouraged to run a risk assessment of the network connections to understand the risk level that a particular power plant may have. Depending on the plant's risk level users are encouraged to take the option of upgrading the HMI Cimplicity system.

Security requires a system approach. HMI CIMPLICITY Systems need to be isolated so that only those computers that need access to the HMIs actually have it. Firewalls and routers are an important aspect to any kind of security system. The plant networks in particular need to control access to port 32000.

The operating system itself is susceptible to various attacks. If these systems are open to actively being patched then the operating systems should have the latest Microsoft ® security updates installed.

Owners of HMI with Windows NT platforms and CIMPLICITY PE Version 4.01 or version 5.5 are encouraged to upgrade hardware systems to a more recent operating system (Windows XP) and move to CIMPLICITY PE version 6.1 and service pack (SP) 6 with Hot Fix. This work should be planned in conjunction with a unit outage of sufficient time. Approximately one (1) day per HMI is required for this work and it may be done in parallel on multiple HMI sites.

Owners with CIMPLICITY 5.5 (non-Windows NT operating systems) should upgrade to SP 3 plus the Hot Fix security software patch. Implementation of this software is estimated at 2 hours per HMI system and this work may be done in parallel on multiple HMI sites.

Owners with CIMPLICITY 6.1 should schedule upgrades to CIMPLICITY 6.1 SP 6 plus Hot Fix security software patch. Implementation of this software fix is estimated at 2 hours per HMI.

Microsoft no longer supports the Windows NT OS (operating system) so there are no security updates available for this latest vulnerability issue. Owners of HMI systems still running the Windows NT OS are encouraged to upgrade their HMI systems. It is important to understand that this recommendation would typically also involve a hardware upgrade of the computer as more recent Windows OS (such as

the suggested Windows XP) require a more powerful computer platform than was required with the Windows NT system.

Contact GE OC-Control Solutions for information on upgrading CIMPLICITY and / or hardware systems.

It is recommended that the customer contact their local GE service office for assistance. GE OC-Control Solutions has developed several upgrade packages depending on computer operating system and Cimplicity Versions for all possible configurations.

This work will require the skills of a Technician knowledgeable with the HMI operating system and the computer Operating System.

Components:

- GE Fanuc CIMPLICITY version 6.1 SP 6 for owners of CIMPLICITY version 4.01 or 5.5 (Windows NT systems will need to be upgraded prior to this software upgrade.)
- Service Pack 3 for CIMPLICITY 5.5 on non-Windows NT systems
- Service Pack 6 for CIMPLICITY 6.1

Estimated time to complete work (depending on scope of work):

- Upgrade Windows Operating System from Windows NT: One day per system.
- Upgrading CIMPLICITY PE Service Pack and Hot Fix only: 2 hours per HMI.

Cause:

The HMI (Human Machine Interface) is the interface between operator and the control system(s). This connection is across a network or networks that may contain both servers and viewers. The HMI is the means by which the operator receives operational data and alarms and issues control commands (see Figure 1). The HMI may also be the workstation that facilitates changes to the control configuration. Due to the nature of networks an HMI may be located anywhere within a plant system but typically one is located near the control panel and another in the control room. The HMI runs on either the Windows NT or Windows XP operating system. This article addresses a vulnerability in the Windows operating system.

This vulnerability was recently reported by US-CERT (United States Computer Emergency Readiness Team) during tests for cyber attack security flaws. Failure to address this issue may result in a corrupted file system on the HMI or a disruption of service resulting in the inability of the HMI to provide the control interface for which it is designed.

It is possible for someone to exploit the vulnerability in communication port use and execute code that could corrupt files and/or affect the HMI operation through a denial of service attack. Although the vulnerability applies only to the HMI it could affect the turbine control panel operation if corrupted files were to be downloaded from the affected HMI to the panel.

“Closed” intranets such as those found on the typical HMI/Turbine network configuration are less exposed to this potential problem. With an Intranet connection the vulnerability is limited due to the limited access this network offers. An attack to this system has to be launched within that local network

(probably limited to the plant system). Added to this is the need for the attacker to be educated on the GE operating system.

On wider-access systems such as internet-similar systems stringent security and administration processes need to be employed. Depending on the presence and location of other HMIs in the plant this may impact the operability of the controlled equipment. This vulnerability exists in all versions of CIMPLICITY HMI versions up to and including version 7.0.

To determine the version of CIMPLICITY in CIMPLICITY project editor (Workbench) click on Help in the menu bar. Click on “About Workbench.” This will detail the version of CIMPLICITY and the Service Pack version currently installed.

With an Internet connection on the HMI the vulnerability of the system increases due to exposure to external systems (see Figure 2). Once into the HMI the attacker is still required to have an understanding of the GE operating system containing the HMI and control configuration files.

If the attacker is successful navigating through these features there is a possibility that the control panel configuration and turbine operation could be compromised if corrupted HMI files are downloaded to the control panel.

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0017630

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.