GE Digital Energy

RSA Private Key & DoS Vulnerabilty

ML800/1200/1600/2400
ML810/3000/3100

Product Bulletin

Date: January 21, 2015 **Classification:** General ICS-CERT Advisory: ICSA-15-013-04

Overview

Two vulnerabilities were identified in GE MultiLink ML800 series managed switches, which, if successfully exploited, could result in unauthorized access and denial of service. GE Digital Energy has validated these vulnerabilities through testing and confirms that the issues affecting the ML800 will also affect the MultiLink series of managed Ethernet switches including the ML1200, ML1600, ML2400, ML810, ML3000, and ML3100. These vulnerabilities have been publicly disclosed.

There are no known public exploits of MultiLink ML800.

This product bulletin discusses the vulnerabilities and provides recommended mitigations.

Background

The MultiLink ML800 is a compact, hardened Managed Ethernet Switch that provides high-speed networking of critical applications, and has been specifically designed for use in industrial facilities, substations and transportation environments.

Researcher Eireann Leverett identified two vulnerabilities associated with the MultiLink ML800 switch and coordinated his findings with GE, the U.S. Department of Homeland Security Industrial Control System – Cyber Emergency Response Team (ICS-CERT) and the UK-CERT. GE has identified mitigation steps to reduce the risk of these vulnerabilities (discussed below) and we are working with our OEM partner to provide a firmware upgrade to address both of these vulnerabilities.

More recently, Mr. Leverett identified a third attack vector, which GE is investigating with his assistance. GE is working to validate that issue and we will provide additional information if and when any vulnerability is confirmed.

Vulnerability Overview

The two confirmed vulnerabilities are: 1) the RSA private key used to decrypt SSL traffic is obtainable from the firmware and 2) the potential for a targeted attack on a specific management interface resulting in sluggish or interrupted (DoS – Denial of Service) communications.

Impact to individual customers depends on many factors that are unique to each customer. GE recommends that customers evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation, and implement the following mitigation measures as appropriate.

Mitigation

Mitigation steps that can be taken immediately

Hard-Coded RSA Private Key

GE encourages our customers to update the switch firmware to the latest published version to enable new keys to be calculated and exchanged. The latest firmware is version5.3.0 for the ML800, ML1200, ML1600 and ML2400 and version 5.3.0.3k for the ML810, ML3000, and ML3100. This firmware is available through the "Resources / Software" link in the product websites (see Appendix A to this Bulletin for a complete list of links). This firmware is also available through the EnerVista Launchpad device management tool. The directions to calculate and exchange keys are in the following table, which will be added to the instruction manuals for the impacted MultiLink switches. It is recommended that the user perform the key exchange over a serial connection to prevent a third party from capturing the new key.

To upload a custom key/certificate file used by SSL	• To upload a custom key/certificate, a user could use the several available file transfer options via CLI (ie: ftp, tftp, xmodem) • Syntax: *ftp get type=cert [ip=<ipaddress>] [file=< cert filename>]* • The key file format used in the MultiLink products is **.pem** • The new key/certificate will permanently overwrite the old key/certificate and it is sustainable through power cycling

Slow data transfer or DoS

This DoS affects the web interface used to configure the device with a web browser. It is recommended that when deploying the device into a production environment that the web server be disabled in order to effectively mitigate this vulnerability. After disabling the web interface a user remains able to configure the device locally or remotely through the command line interfaces without risk of exploitation.

By connecting to the command line interface through either a serial connection or through telnet it is possible to disable the web server with the following commands:

```
ML800# access
ML800(access)## web disable
```

This change may be verified by using the `show web` command:

```
ML800(access)## show web
  HTTP is disabled.
```

Save the configuration to maintain this new setting.

General mitigation measures

GE recommends its customers implement network security defensive measures to minimize risk of their network being compromised, including:

- Minimize network exposure to all other control system devices. Control system devices should not be connected directly to the internet.
- Locate control system network(s) and devices behind properly configured firewalls, and isolate them from the business network.
- Utilize detection methods to monitor for anomalous network traffic that is "out of band" and not expected.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs) recognizing that the VPN is only as secure as the connected devices.

Future Firmware Upgrade from GE

GE has worked with its OEM partner to develop a new firmware version that removes the hard-coded RSA private key, and that provides a fix to the web server. This firmware version is going through production testing and verification. When available, the upgraded firmware will be released through the GE Digital Energy website and the EnerVista Launchpad tool. Instruction manuals for the MultiLink switches will be updated and released through the website and EnerVista Launchpad.

Acknowledgements

GE would like to thank Eireann Leverett for reporting these issues to GE, ICS-CERT and UK-CERT, assisting GE in its investigation, and helping to protect GE customers.

****

GE 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 the PSIRT at www.ge.com/security or security@ge.com.

Product Support

GE Digital Energy is committed to the continued support of the MultiLink product line. We appreciate your business and look forward to continuing to grow our relationship.
If you need help with any aspect of your GE Digital Energy product, you have a few options:

Search Technical Support

The GE Digital Energy Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics. Visit us on the Web at: **http://www.gedigitalenergy.com/**

Contact Customer Service

The GE Digital Energy Customer Service Center is open 24 hours a day, seven days a week for you to talk directly to a GE representative.
In the U.S. and Canada, call toll-free: 1-800-547-8629
International customers please call: + 1-905-294-6222
Or e-mail to: **ge4service@ge.com**