GE Digital Energy

RSA Private Key & DoS Vulnerabilty

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

Product Bulletin

Date: January 6, 2015 **Classification:** General ICS-CERT Advisory: ICSA-15-013-04
Updated: September 8, 2015
GE Publication Number: GET-20024A

Overview

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

This product bulletin discusses the vulnerabilities, announces the release of firmware versions that eliminates the vulnerabilities, and provides additional recommended mitigations. Multiple vulnerabilities described in this bulletin have been resolved in version 5.3.0 of the firmware, released on January 21st, 2015. GE has updated this product bulletin to inform its customers of the release of a tool illustrating the Denial of Service vulnerability.

Background

The MultiLink ML800 is a compact, hardened Managed Ethernet Switch. It 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) as well as resolution to these vulnerabilities in firmware version 5.3.0 for the ML800, ML1200, ML1600 & ML2400; and firmware version 5.3.2-3K for the ML810, ML3000 & ML3100.

Additionally, Mr. Leverett assessed the web interface hosted by the ML800 and determined it was susceptible to cross-site scripting. GE has resolved these cross-site scripting vulnerabilities in firmware version 5.3.2-3K for the ML810, ML3000 & ML3100.

Vulnerability Overview

The three confirmed vulnerabilities are: 1) the RSA private key used to decrypt SSL traffic is obtainable from the firmware, 2) the potential for a targeted attack on a specific management interface resulting in sluggish or interrupted (DoS – Denial of Service) communications, and 3) the potential for crafted web requests to inject content into response pages (cross-scripting) from the web interface.

Mitigation

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. This issue was resolved in firmware version 5.3.0 for the ML800, ML1200, ML1600 and ML2400; and firmware version 5.3.2-3K for the ML810, ML3000 & ML3100, which is available for download through the "Resources / Software" link in the product websites at:

http://www.gedigitalenergy.com/multilin/catalog/ml800.htm

This firmware is also available through the EnerVista Launchpad device management tool.

Slow data transfer or DoS

The DoS vulnerability affected the web interface used to configure the device with a web browser. This issue was resolved in firmware version 5.3.0 for the ML800, ML1200, ML1600 and ML2400; and firmware version 5.3.2-3K for the ML810, ML3000 & ML3100.

Cross-site scripting vulnerabilities

The identified cross-site scripting vulnerabilities allow a user to inject arbitrary web content into specific pages within the web interface. A malicious actor could use this vulnerability to craft a link that exposes another user of the ML800 web interface to web content not generated by the device. This issue is resolved in firmware version 5.3.2-3K for the ML810, ML3000 & ML3100. Users of the ML800, ML1200, ML1600 & ML2400 should follow the alternative mitigations strategy referenced below until firmware version 5.3.2 is released for these devices.

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.

Alternative Mitigations

The following mitigations are provided in case it is not possible to update a device in order to mitigate the above vulnerabilities. GE recommends that a user update the firmware where possible.

Hard-Coded RSA Private Key

It is possible to override the RSA Private key utilized by the ML800. The directions to calculate and exchange keys are in the following table, which are included within 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. It is not necessary for a user to perform these steps if the device has been updated to firmware version 5.3.0 or newer, since a new certificate will be generated during the update process.

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, sftp) • 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

It is possible to mitigate this vulnerability by disabling the web server that provides the web configuration interface. 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.

Cross-site scripting vulnerabilities

It is possible to mitigate this vulnerability by disabling the web server that provides the web configuration interface. 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.

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**