SIEMENS

Upgrading OpenSSL on RUGGEDCOM APE to Fix the Heartbleed Vulnerability AN25

Application Note

4/2014
RC1150-EN-02

Disclaimer Of Liability

Siemens has verified the contents of this manual against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

ROX™, Rugged Operating System On Linux™, CrossBow™ and eLAN™ are trademarks of Siemens Canada Ltd. . ROS® is a registered trademark of Siemens Canada Ltd..

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens ' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Contacting Siemens

Address	Telephone	E-mail
Siemens Canada Ltd. Industry Sector 300 Applewood Crescent Concord, Ontario Canada, L4K 5C7	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288 Fax: +1 905 856 1995	ruggedcom.info.i-ia@siemens.com **Web** www.siemens.com/ruggedcom

Table of Contents

Preface

This application note is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for us by network and system planners, system programmers, and line technicians.

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM APE User Guide*

Accessing Documentation

The latest Hardware Installation Guides and Software User Guides for most RUGGEDCOM products are available online at www.siemens.com/ruggedcom.

For any questions about the documentation or for assistance finding a specific document, contact a Siemens sales representative.

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens sales representative.

Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, please contact Siemens Customer Support through any of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens's extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community via the forum
  - And much more...

1 Introduction

As of 1 February 2014, Siemens has been shipping some Linux® variants of RUGGEDCOM APE line modules (order codes APE1402-XX, APE1402-C01, APE1404-XX, and APE1404-C01, or MFLBs 6GK6015-0AL20-0GB0, 6GK6015-0AL20-0GB1, 6GK6015-0AL20-0GD0, and 6GK6015-0AL20-0GD1) with a version of the OpenSSL cryptographic software library that is vulnerable to the Heartbleed [http://www.heartbleed.com] security vulnerability.

In response to the severity of the Heartbleed vulnerability, Siemens strongly recommends that customers of RUGGEDCOM APE line modules follow the procedures described in this application note to upgrade the OpenSSL package, if necessary, regardless of the manufacturing date of their hardware.

The following sections describe in further detail how to upgrade OpenSSL on a RUGGEDCOM APE line module:

- Chapter 2, *Verifying the OpenSSL Version*
- Chapter 3, *Upgrading OpenSSL*

2 Verifying the OpenSSL Version

To determine the version of OpenSSL currently installed, do the following:

1. Log in or gain root access to the APE line module.
2. At the command prompt, type the following command:

   ```
   dpkg -l openssl
   ```

If the version is *1.0.1e-2+deb7u4*, the OpenSSL cryptographic software library is vulnerable to Heartbleed.

3 Upgrading OpenSSL

There are two methods available for upgrading the OpenSSL cryptographic software library.

Method 1: Obtaining an Upgrade Package from the Debian Security Update Repository

1. Make sure the APE module has access to the Internet.
2. Log in or gain root access to the APE line module.
3. Using vim or nano, open the file /etc/opt/sources.list and add the following line:

   ```
   dep http://security.debian.org wheezy/updates main
   ```

   This points Debian's upgrade system (referred to as *APT*) to Debian's online Security Update Repository for Debian 7. APE line modules based on Debian 6 are not vulnerable to Heartbleed and require no update.
4. At the command prompt, type the following commands to upgrade the OpenSSL cryptographic software library:

   ```
   apt-get update
   apt-get install openssl libssl1.0.0
   ```

   Make sure both commands execute without errors.
5. Make sure OpenSSL has been upgraded to version 1.0.1e-2+deb7u6 or later. For more information, refer to Chapter 2, *Verifying the OpenSSL Version*.
6. If further security updates from Debian's Security Update Repository are not desired, remove the lines previously added to /etc/apt/sources.list.

Method 2: Obtaining an Upgrade Package from Siemens Customer Support

1. Request the following Debian packages from Siemens Customer Support:
   - openssl_1.0.1e-2+deb7u6_i386.deb
   - libssl1.0.0_1.0.1e-2+deb7u6_i386.deb
2. Once obtained, upload the files to the APE line module via SFTP, SCP or a USB memory media.
3. Log in or gain root access to the APE line module.
4. At the command prompt, type the following command to upgrade the OpenSSL cryptographic library:

   ```
   dpkg -i openssl_1.0.1e-2+deb7u6_i386.deb libssl1.0.0_1.0.1e-2+deb7u6_i386.deb
   ```

5. Delete the .deb files by typing:

   ```
   rm openssl_1.0.1e-2+deb7u6_i386.deb libssl1.0.0_1.0.1e-2+deb7u6_i386.deb
   ```