SIEMENS

FAQ • 07/2014

Upgrading OpenSSL - Security Advisory SSA-635659

RUGGEDCOM APE (Linux® Versions Only)

http://support.automation.siemens.com/WW/view/en/97664169

Warranty and liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these application examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens Industry Sector.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, 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.

Table of contents

1 Introduction

The following RUGGEDCOM APE line modules may be open to vulnerabilities related to certain versions of OpenSSL (CVE-2014-0160), specifically the Heartbleed vulnerabitlity:

Order Code	MFLB
APE1402-XX	6GK6015-0AL20-0GB0
APE1402-C01	6GK6015-0AL20-0GB1
APE1404-XX	6GK6015-0AL20-0GD0
APE1404-C01	6GK6015-0AL20-0GD1

In response to the severity of these vulnerabilities, Siemens strongly recommends that customers of RUGGEDCOM APE line modules follow the prescribed process to upgrade the OpenSSL packages, 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:

- Verifying the Software Version
- Upgrading Software

2 Verifying the Software Version

To determine the version of OpenSSL currently installed on your RUGGEDCOM APE line module, do the following:

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

```
dpkg -l openssl
```

If the version is less than or equal to *1.0.1e-2+deb7u4*, the OpenSSL cryptographic software library is vulnerable.

3 Upgrading Software

NOTICE	**Security Hazard** Do not connect the APE module to the Internet outside of a secure network perimeter. Make sure a firewall is configured for the host RX15xx device.

1. Make sure the APE module is connected to the Internet via the RX15xx device.
2. Log in or gain root access to the APE module.
3. Using a text editor such as **vim** or **nano**, open the file */etc/apt/sources.list* and add the following lines:

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

   This points Debian upgrade system (referred to as APT) to Debian online Security Update Repository for Debian 7.
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
   ```

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

4 Related literature

	Topic	Title / Link
\1\	Siemens Industry Online Support	http://support.automation.siemens.com
\2\	Download page of this entry	http://support.automation.siemens.com/WW/view/en/97664169
\3\	RUGGEDCOM APE User Guide	http://support.automation.siemens.com/WW/view/en/81193317

5 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 one 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’ 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…

6 History

Version	Date	Modifications
V1.0	07/2014	First version