



Luna Appliance Bash Vulnerability

PATCH NOTE

Document applies to patch part number: 630-010386-001

Document revision: Rev D

Patch note issued on: 01 October 2014

Patch Description

This patch addresses vulnerabilities with all versions of the BASH Shell known as “ShellShock” and “AfterShock”. Exploitation of this vulnerability could allow for the unauthorized execution of arbitrary code. Details can be found at:

- CVE-2014-6271 (<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271>)
- CVE-2014-7169 (<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169>)

Only authenticated users of the Luna SA/SP appliance administration service could use this vulnerability to execute unintended commands on the appliance. In addition, if DHCP services have been enabled, an unauthenticated user on the local network could execute unintended commands.

SafeNet recommends that you install this patch immediately on all affected appliances.

CAUTION: This patch does not survive a software upgrade. If you upgrade your appliance software after installing this patch, you must reapply this patch after the upgrade is complete.

Products Affected

- Luna SA 5.x
- Luna SP 3.x

WARNING! This patch applies only to the products listed above. Do not install this patch on any other products or versions. Installing this patch on any other product may require RMA.

Preparing to Install the Patch

Before attempting to install the patch, ensure that you have satisfied the following prerequisites:

- you have the patch file (.tar) that contains the patch file and authorization code.
- you have prepared your appliance for the upgrade ensure a successful, trouble-free, installation.

To prepare to install the patch

1. Copy the patch file (.tar) to the Luna client computer that is connected to the appliance you want to update.
2. Use your favorite archiving program to untar the archive.
3. Ensure that your appliance is connected to an uninterruptable power supply (UPS).
4. Backup the contents of your HSM partitions to Luna Backup HSMs.
5. Stop all client applications that are using the HSM appliance.

Installing the Patch

The patch is delivered as a secure package update that you securely copy to the appliance and then install using the **package update** command.

To install the appliance patch

1. Copy the secure package update file (.spkg) to the Luna appliance you want to upgrade:

Windows	pscp <path>\<secure_package_update>. spkg admin @<appliance_IP_or_hostname>:
Unix/Linux	scp <path>/<secure_package_update>. spkg admin @<appliance_IP_or_hostname>:

2. At the console, log in to the Luna appliance using an admin-level account (the default account is admin).
3. Log in to the Luna HSM as the HSM Admin or Security Officer user:

```
lunash:> hsm login
```

For a Luna appliance with PED authentication, the blue PED Key is required. For a Luna appliance with password authentication, you are prompted for the HSM Admin (SO) password.

4. Verify that the upgrade package file that you copied is present (optional):

```
lunash:> package listfile
```

5. Verify the upgrade package (optional):

```
lunash:> package verify <secure_package_update>.spkg -authcode <authorization_code>
```

6. Install the upgrade package:

```
lunash:> package update <secure_package_update>.spkg -authcode <authorization_code>
```

Note: The authorization code is supplied as a text file. Simply read the file and type the contained code into your command. Do not upload the authcode file.

During the installation process, a series of messages are displayed that detail the progress of the upgrade.

8. Reboot the Luna appliance.
9. Restart and reconnect all services and client applications.

Verifying the Installation

After you install the patch, it is recommended that you verify that it installed successfully.

To verify that the patch is installed

1. At the console, log in to the Luna appliance using an admin-level account (the default account is admin).
2. Log in to the Luna HSM as the HSM Admin or Security Officer user :

```
lunash:> hsm login
```

For a Luna appliance with PED authentication, the blue PED Key is required. For a Luna appliance with password authentication, you are prompted for the HSM Admin (SO) password.

3. Verify that the package is installed:

```
lunash:> package list
```

Scan the output of the command for the following string:

```
bashupgrade-1.0.0-<n>
```

where <n> is an integer.

Technical Support Information

If you have questions or need additional assistance, contact Technical Support through the listings below:

Contact method	Contact information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	(800) 545-6608, (410) 931-7520
	Australia and New Zealand	+1 410-931-7520
	China	(86) 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	India	+1 410-931-7520
	United Kingdom	0870 7529200, +1 410 931-7520
Web	www.safenet-inc.com/Support	
Support and Downloads	www.safenet-inc.com/Support Provides access to the SafeNet Knowledge Base and quick downloads for various products.	
Customer Technical Support Portal	https://serviceportal.safenet-inc.com Existing customers with a Customer Connection Center or Service Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	

Trademarks and Disclaimer

Although we have attempted to make this document as complete, accurate, and useful as possible, we cannot guarantee its contents. Errors or omissions will be corrected, as they are identified, in succeeding releases of the product. Information is subject to change without notice.

Copyright 2014. All rights reserved.

Luna and the SafeNet logos are registered trademarks of SafeNet, Inc.