X-Series customers are advised to upgrade to XOS V10.0.2.0, XOS V9.7.5.0, XOS V9.6.9.0, or XOS V9.5.7.0 as soon as possible to address the recently discovered “Shellshock” vulnerabilities in the GNU Bourne Again shell (Bash) command interpreter used in Linux systems. Please refer to Blue Coat Security Advisory SA82 for more information on Shellshock.

Customers who cannot upgrade immediately may use the patched RPMs available from Blue Touch Online (BTO) located at https://bto.bluecoat.com to update their systems. Patched RPMs are available for XOS branches 10.0.x, 9.7.x, 9.6.x, and 9.5.x. Customers running an XOS version prior to XOS V9.5 are advised to upgrade to XOS V10.0.2.0, XOS V9.7.5.0, XOS V9.6.9.0, or XOS V9.5.7.0 as soon as possible.

1.0 Updating Bash on the X-Series

To update Bash on the X-Series Platform, download the TGZ file bash_xseries_95x_96x_97x_10x.tgz from the X-Series Support Portal. Untar the file.

The TGZ archive contains the following patched Bash RPM files.

<table>
<thead>
<tr>
<th>RPM Version</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash-3.2-33.el5_11.4.x86_64.rpm</td>
<td>For CPMs and xslinux_v5_64 or xsve VAP groups</td>
</tr>
<tr>
<td>bash-3.2-33.el5_11.4.i386.rpm</td>
<td>For xslinux_v5 VAP groups</td>
</tr>
</tbody>
</table>

Follow the instructions below to update the Bash RPMs X-Series Platform.

**IMPORTANT:** Updating the Bash RPMs on the X-Series Platform requires two procedures.

1. Update the Bash RPMs on all CPMs.
2. Update the Bash RPMs on all VAP groups.
1.1 Updating the Bash RPMs on X-Series CPMs

Use the bash-3.2-33.el5_11.4.x86_64.rpm version of the patched RPMs to update Bash on CPMs.

1. Use the following command to verify that the version of XOS running on the system is supported for a manual Bash RPM update. Only XOS branches 10.0.x, 9.7.x, 9.6.x, and 9.5.x are supported for manual update of Bash.

   CBS# show version

2. Copy the patched bash-3.2-33.el5_11.4.x86_64.rpm file to the CPM.

3. Log on to the Unix prompt with root privileges.

4. Run the following command to determine the version of Bash installed.

   [root@xxxx admin]# rpm -q bash
   bash-3.2-32.el5_11.4.x86_64.rpm

   The version bash-3.2-32 shown in the output is not a patched version.

5. Run the following command to update Bash to the patched version.

   [root@xxxx admin]# rpm -Uh bash-3.2-33.el5_11.4.x86_64.rpm

6. Run the following command to verify that the patched RPM is installed.

   [root@xxxx admin]# rpm -q bash
   bash-3.2-33.el5_11.4.x86_64

   The output in the example above indicates that the patched version is installed.

7. Run the following command to verify that the patched RPM is being used on the system.

   [root@xxxx admin]# env x='()' { ; }; echo vulnerable' bash -c 'echo hello'
   hello

   If the word "vulnerable" had printed in the example above, it would mean that Bash had not been patched successfully.

8. Repeat these steps for each CPM in the system.

NOTE: To view the upgrade status of the Bash and other RPMs on the system, run the show current-release verify-rpm CLI command.

CBS# show current-release verify-rpm
Copyright (c) 2000-2014 by Blue Coat Systems, Inc. All rights reserved.Version: XOS 10.0.1 [Jul 29 2014 05:12:10] (bldmnr) gcc: gcc version 2.96 20000731 (Linux 7.3 2.96-112) CVS_Label: XOS-10_0_1_0-20140729_1 Kit_Number: 22

Upgraded rpm: bash-3.2-33.el5_11.4 x86_64 from: bash-3.2-32.el5 64 bit on CPM
1.2 Updating the Bash RPMs on X-Series VAP Groups

Check Point Applications

IMPORTANT: X-Series customers running Check Point applications must obtain a patched version of Bash from Check Point Support to resolve the Shellshock vulnerability. Follow Check Point's instructions to install the patch. For more information, see the Check Point Secure Knowledge Base article sk102673.

Imperva, Sourcefire, and McAfee Applications

X-Series customers running applications from Imperva, Sourcefire, or McAfee may use the following procedure to update Bash for VAP groups.

NOTE: In addition to installing the XOS patch, McAfee customers should contact McAfee Customer Support for a resolution of the Shellshock vulnerability on the McAfee application.

Use the patched Bash RPM that corresponds to your VAP group operating system to update Bash on each VAP group member and on the VAP common image.

- For xslinux_v5 VAP groups, use bash-3.2-33.el5_11.4.i386.rpm
- For xslinux_v5_64 or xsve VAP groups, use bash-3.2-33.el5_11.4.x86_64.rpm

Updating Bash on the VAP common image is required to ensure that new members added to the VAP group by incrementing the VAP count include the patched Bash RPM.

IMPORTANT: If you later create a new VAP group, all VAP members and the VAP common image of the new VAP group must be patched.

The following instructions assume you have copied the required patched Bash RPM file(s) to the system and that the file(s) are in the default (#tftpboot/.private/home/admin) directory.

1. Verify the VAP group operating system and number of VAP members.

   CBS# show running-config vap-group test
   vap-group test xslinux_v5_64
   vap-count 2

   In this example, the VAP group named test contains two VAP members and uses the xslinux_v5_64 VAP OS. You must manually update the Bash RPM on each VAP member and on the VAP common image.

2. Log on to the Unix prompt with root privileges.

3. Run the following commands to determine the version of Bash installed on each VAP member and on the VAP common image.

   [root@xxxx admin]# rpm -q --root /tftpboot/test_1/ bash
   bash-3.2-32.el5.x86_64

   [root@xxxx admin]# rpm -q --root /tftpboot/test_2/ bash
   bash-3.2-32.el5.x86_64

   [root@xxxx admin]# rpm -q --root /tftpboot/test_common/ bash
   bash-3.2-32.el5.x86_64

   The version bash-3.2-32 shown in the output is not a patched version.
Updating Bash on the X-Series Platform

4. Run the following commands to update Bash to the patched version on each VAP member and on the VAP common image.

   [root@xxxx admin]# rpm -Uh --root /tftpboot/test_1/ bash-3.2-33.el5_11.4.x86_64.rpm
   [root@xxxx admin]# rpm -Uh --root /tftpboot/test_2/ bash-3.2-33.el5_11.4.x86_64.rpm
   [root@xxxx admin]# rpm -Uh --root /tftpboot/test_common/ bash-3.2-33.el5_11.4.x86_64.rpm

   **NOTE:** You can safely ignore the DSA signature warning that may appear.

5. Run the following commands to verify that the patched RPM is installed on each VAP member and on the VAP common image.

   [root@xxxx admin]# rpm -q --root /tftpboot/test_1/ bash
   bash-3.2-33.el5_11.4.x86_64
   [root@xxxx admin]# rpm -q --root /tftpboot/test_2/ bash
   bash-3.2-33.el5_11.4.x86_64
   [root@xxxx admin]# rpm -q --root /tftpboot/test_common/ bash
   bash-3.2-33.el5_11.4.x86_64

   The output in the example above indicates that the patched version (bash-3.2-33) is installed.

6. To verify that the patched RPM is being used on each VAP member, use rsh to connect to the VAP member (for example, test_1) and run the following command.

   [root@xxxx admin]# rsh test_1
   test_1 (xxxx): ~# env x='()' {} ;; echo vulnerable' bash -c 'echo hello'
   hello

   If the word "vulnerable" had printed in the example above, it would mean that Bash had not been patched successfully on the VAP member.

   **IMPORTANT:** Remember, if you create new VAP groups in the future, you must patch Bash on all VAP members and on the VAP common image.
2.0 X-Series Customer Support

Blue Coat Systems offers a variety of service plans designed to meet your specific technical support requirements. For information on purchasing a service plan for your organization, please contact your account representative or refer to Blue Touch Online (BTO) located at https://bto.bluecoat.com. If you have purchased a product service plan and need technical assistance, you can report issues by telephone. For the current list of regional customer support phone numbers, see: http://www.bluecoat.com/support/contactsupport/.

All of our service plans include access to Blue Touch Online. Blue Touch Online provides you with access to a variety of resources, including Customer Support Knowledgebase articles, technical bulletins, product documentation, and release notes. You can also access our real-time problem reporting application, which lets you submit new technical support requests and view all your open requests.

Blue Coat Systems also offers extensive customer training on all of its products. For current course offerings and schedules, please refer to the X-Series Training Services Web pages located at http://www.bluecoat.com/support/training/x-series-training-services.

Copyright and Trademark Information

© 2014 by Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHES, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING. SECURITY EMPOWERS BUSINESS, BLUETOUGH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only. BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas: Blue Coat Systems, Inc. 420 N. Mary Ave. Sunnyvale, CA 94085

Rest of the World: Blue Coat Systems International SARL 3a Route des Arsenaux 1700 Fribourg, Switzerland

3.0 Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 8, 2014</td>
<td>First release.</td>
</tr>
</tbody>
</table>