WatchGuard® XCS v10.0 Hotfix 2 Release Notes

WatchGuard XCS Build	140409
Revision Date	April 11, 2014

Introduction

This hotfix release updates an OpenSSL library to resolve the "Heartbleed" OpenSSL vulnerability. Even without this patch, the WatchGuard XCS is not vulnerable to attack. Most SSL-encrypted services of the WatchGuard, including all inbound services, use an earlier non-vulnerable version of OpenSSL. The vulnerable OpenSSL library is used only for communications between the WatchGuard XCS appliance and Voltage, our SecureMail encryption provider. The WatchGuard XCS acts as a client for these connections, not a listening server. The OpenSSL vulnerability can only be exploited on the server side, and we believe there is no risk to the WatchGuard XCS, including SecureMail users.

This release also contains defect fixes for the Centralized Management and Tiered Admin features.

For full information, see the Resolved Issues section.

Before You Begin

Before you install this update release:

- Read the information in the Known Issues and Limitations section of these Release Notes.
- For more information about how to configure WatchGuard XCS, from the Web UI, select **Support > Online Manual**.
- The latest versions of the product documentation are available at www.watchguard.com/help/documentation.

Download Software

If Security Connection is enabled, the software update is downloaded automatically to your XCS device. The update is not automatically installed. You must manually install software updates on the **Software Updates** page.

See the *Install the Software Update* section below for detailed instructions.

To download the software manually:

1. Go to http://www.watchguard.com/archive/softwarecenter.asp.
2. Log in to the WatchGuard Portal and click the **Articles & Software** tab.
3. Search to see all available **Software Downloads** articles and find the **WatchGuard XCS Software Downloads** article.
4. Select and download the WatchGuard XCS v10.0 Hotfix 2 software. The file is called *xcs100_hotfix_2.pf*.

Install the Software Update

To install this update release:

Back Up the WatchGuard XCS Configuration

1. Select **Administration > Backup/Restore > Backup and Restore.**
2. Select your backup method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
3. Select which information to back up. If you do not want to restore reporting data, clear the **Backup reporting db data** check box. We recommend you select all options.

   For the **FTP** and **SCP** methods, enter your server information.
4. Click **Next** to confirm your selections.
5. Click **Create backup now**.

Install the Software Update

1. Select **Administration > Software Update > Updates**.
2. If you use Security Connection, the software update already appears in the **Available Updates** section.

   If you manually downloaded your software update:

   - Click **Browse** and select the software update.
   - Click **Upload**.
3. In the **Available Updates** section, select the software update.
4. Click **Install**.
   The device will restart when the installation is complete. This process may take several minutes.

To Install the Software Update in a Cluster

1. On all devices in the cluster, change the cluster run mode to **Standalone** mode.

We recommend that you stop message processing on any **Client** systems before you switch them to **Standalone** mode. This prevents the system from processing mail with a default configuration when you change the mode back to **Client**. The **Client** needs time to update its configuration from the **Primary** system when the **Client** is added to the cluster again after the update.

2. Install the update on the **Primary**, and then restart the device.
3. Change the run mode of the **Primary** device from **Standalone** back to **Primary** mode.
4. Install the update on the **Secondary**, and then restart the device.
5. Change the run mode of the **Secondary** system from **Standalone** back to **Secondary** mode.
6. Install the update on any **Client** devices, and then restart the device.
7. Change the run mode of the **Client** devices from **Standalone** back to **Client** mode.

Resolved Issues

- Centralized Management configuration synchronization now works properly on the CM Manager system. *[79305]*
- Error messages no longer appear on the CM Manager system after a Centralized Management configuration synchronization. *[79975]*
- Dashboard content now loads properly when logged in as a Tiered Admin user. *[79921]*
- This release includes an update to the OpenSSL libraries in response to the reported "Heartbleed" vulnerability (CVE-2014-0160). *[80014]*

Known Issues and Limitations

There are no known issues in this release.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375