WatchGuard® XCS v10.2 Release Notes

WatchGuard XCS Build	250118
Release Date	February 12, 2018
Release Notes Revision Date	June 5, 2018

After you install WatchGuard XCS v10.2, make sure you install any additional software updates available for this release.

See these release notes for information about updates to WatchGuard XCS v10.2:

- WatchGuard XCS v10.2 Update 1 Release Notes

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.2. This release is a security update only and does not contain any new features, enhancements, or resolved issues.

This release addresses these security issues:

FreeBSD

CVE-2016-6559: The BSD libc library's link_ntoa() function may be vulnerable to a classic buffer overflow. It is currently unclear if this issue is exploitable. See FreeBSD-SA-16:37.libc.

OpenSSL

CVE-2016-2177: OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.

CVE-2016-2178 The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.

CVE-2016-2179: The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.

CVE-2016-2180: The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.

CVE-2016-2181: The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.

CVE-2016-2182: The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.

CVE-2016-6302: The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.

CVE-2016-6303: Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.

CVE-2016-6304: Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

CVE-2016-6306: The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

CVE-2016-7052: crypto/x509/x509_vfy.c in OpenSSL 1.0.2i allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) by triggering a CRL operation.

CVE-2016-7055: There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.0 before 1.1.0c that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible.

CVE-2017-3731: If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash.

CVE-2017-3732: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely.

NTP

CVE-2016-7426: NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address.

CVE-2016-7427: The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via a crafted broadcast mode packet.

CVE-2016-7428: ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via the poll interval in a broadcast packet.

CVE-2016-7431: NTP before 4.2.8p9 allows remote attackers to bypass the origin timestamp protection mechanism via an origin timestamp of zero. NOTE: this vulnerability exists because of a CVE-2015-8138 regression.

CVE-2016-7433: NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."

CVE-2016-7434: The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.

CVE-2016-9310: The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.

CVE-2016-9311: ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.

CVE-2017-6464: NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.

CVE-2017-6462: Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.

CVE-2017-6463: NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service (daemon crash) via an invalid setting in a :config directive, related to the unpeer option.

CVE-2016-9042: A vulnerability was found in NTP, affecting the origin timestamp check function. An attacker able to spoof messages from all of the configured peers could send crafted packets to ntpd, causing later replies from those peers to be discarded, resulting in denial of service.

OpenSSH

CVE-2016-6515: The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

CVE-2016-8858: The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."

CVE-2016-10009: Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

CVE-2016-10010: sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.

Before You Begin

Before you install this update release, please note these considerations.

About WatchGuard XCS v10.2 and System Resources

- WatchGuard XCS v10.2 requires more memory than previous versions, and WatchGuard recommends a minimum of 4GB.
- Do not upgrade WatchGuard XCS hardware models that have 2GB memory or lower such as the XCS170 or XCS370.
- The VMWare virtual machine file *XCS-102.ova* is pre-configured with 4GB memory by default.
- The Hyper-V virtual machine must be configured with a minimum of 4GB memory.
- Make sure you back up your system before you perform a full system upgrade. Before you back up the system, WatchGuard recommends you reduce the amount of quarantined mail in your quarantine, or do not back up any quarantined mail. This reduces the size of your backup and prevents resource issues during an upgrade.

Downgrade Notes

You cannot downgrade a system from XCS v10.2 to XCS v10.0 with a *.pf* package. In this case you must use the console installation method. For details on how to install a software upgrade from the console, see Install the Software.

Resources

- 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 https://www.watchguard.com/wgrd-help/documentation/overview.

Download Software

To download the software:

1. Go to http://software.watchguard.com.
2. Select and download the appropriate WatchGuard XCS v10.2 software package:

- **xcs102_upgrade.pf** — This is a software update file that you can upload directly to the XCS on the Software Updates page.
  - This is the recommended method to upgrade to v10.2.
  - You must be running WatchGuard XCS v10.0 Update 3 or higher to use this software upgrade method.
  - This method can be used for both XCS and XCSv.
- **xcs-102.zip** — This package contains an upgrade image file (.img) and the BTIweb software so you can perform a network image upgrade from the system console.
  - This method requires a minimum version of WatchGuard XCS v9.2 Update 5 or higher.

- **XCSv-102.ova** — This package contains an OVA template for an installation of XCSv v10.2 on VMware.
- **XCSv-102-HyperV.zip** — This package contains the files required to install XCSv v10.2 on Microsoft Hyper-V.

Install the Software

There are two ways to install the XCS v10.2 software:

- Install the Software Upgrade from the Web UI — Use the software upgrade file packaged as a software update *(xcs102_upgrade.pf)*. You can install this file from the Software Updates page on the Web UI. You must be running WatchGuard XCS v10.0 Update 3 or higher to use this software upgrade method. This method can be used for both XCS and XCSv.
- Install the Software Upgrade from the Console — Use the full software image file *(xcs-102.img)* for a network upgrade installation from the system console. This method requires a minimum version of WatchGuard XCS v9.2 Update 5 or higher.

We recommend that you use the Web UI to upload the *xcs102_upgrade.pf* file on the Software Updates page to install this upgrade. This method preserves your system IP address and network information, admin login name and passwords, time zone information, and feature key. As part of the upgrade process, you will also be prompted to backup and restore your configuration.

If you install a full system upgrade, your current configuration and data will be deleted. Make sure you perform a backup of your system before you perform a full system upgrade.

Back Up the WatchGuard XCS Configuration

Make sure you back up your system before you perform a full system upgrade. Before you back up the system, WatchGuard recommends you reduce the amount of quarantined mail in your quarantine, or do not back up any quarantined mail. This reduces the size of your backup and prevents resource issues during an upgrade.

To perform a backup:

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 back up and restore reporting data or quarantined mail, clear the **Backup reporting db data** and **Backup Quarantine mail** check boxes.

   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 Upgrade from the Web UI

You can install a full system upgrade from the **Software Updates** page. The upgrade is distributed as a *.pf* file just like a software update. When you upload a full system software upgrade, it appears in the *System Upgrades* section. When you perform a system upgrade, the system retains its original IP address and network settings, time zone, admin user logins and passwords, and feature key information. When the system restarts, you can connect to the system using its original IP address. You can then perform a restore of your configuration from backup.

ⓘ You must be running WatchGuard XCS v10.0 Update 3 or higher to use this software upgrade method.

- This upgrade method requires that you have at least 2 GB free space in the *System Data Storage* disk area. To check your free disk space, select **Activity > Dashboard > System Summary > Disk Usage**.
- Any network interface specific features that you enabled before the upgrade (for example: Large MTU, Respond to Ping, Trusted Subnet, Admin & Web User Login, WebMail, SNMP Agent, Centralized Management, HTTP/HTTPS Proxy, Queue Replication, Bridging, and Transparent Mode) will be reset to the default setting. You must re-enable these options after the upgrade is complete.
- Cluster status is preserved, but the system will restart in Standalone mode after the upgrade. You must manually change the run mode to the system's previous mode, such as Primary, Secondary, or Client.

To install the software upgrade from the Software Updates page on the Web UI:

1. Select **Administration > Software Update > Updates**.
   The Software Updates page appears.
2. Click **Browse** and select the software upgrade file. The file name is `xcs102_upgrade.pf`.
3. Click **Upload**.
   The software update appears in the System Upgrades section.
4. In the **System Upgrades** section, select the software upgrade you want to install.
5. Click **Upgrade**.
   You will be prompted to perform a backup of your system. After you install the software upgrade, you must restart the device.

ⓘ The installation process can take several minutes to complete. The system will reboot three times before you will be able to access it via the Web UI.

6. Log in to the system as the primary admin user.
   You will be prompted to perform a restore of your configuration.
7. Select your restore method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
8. Select which information to restore.
   For the FTP and SCP methods, enter your server information.
9. Click **Next** to confirm your selections.
10. Click **Restore now**.

Reapply Network Settings

To make sure that your network settings are correctly applied after you upgrade the device and restore your configuration, you must reapply the network settings.

1. Select **Configuration > Network > Interfaces**.
2. Click **Apply**.
3. After you apply the settings, you must reboot the XCS device.

Install the Software Upgrade from the Console

To install the software upgrade from the system console using a *.img* file:

> You must be running WatchGuard XCS v9.2 Update 5 or higher to use this software upgrade method.

Install and Run BTIweb

BTIweb is a small web server that hosts the software image file for a network upgrade installation.

1. On your local workstation, extract the files from the *xcs-102.zip* archive.
2. In the *btiweb* directory, double-click **btiweb.exe**.
3. To start the web server service, click **Start**.

Install the Software Upgrade from the Console

1. Attach a monitor and keyboard (PS/2 or USB) to the connectors on the back panel of your XCS device.
2. Log in to the console.
3. Select **Admin > Reboot**, and then select **Yes** to confirm.
4. When the device restarts, press **F1** to start the installation process.
5. Press **Enter**.
6. Select your **Keyboard Type** for your location.
7. Select **Auto**, and then select **OK**.
8. Select **Network**.
9. Configure the settings for the first network interface of your device.
10. In the **Install Path** field, type the URL of the computer on which you installed BTIweb. For example, `http://10.0.0.2/`
    Make sure you type the trailing "/" character.
11. Select **xcs-102.img**.
12. Select **Save Image to Hard Disk**.
    The software image is copied to the local disk.
13. Press **Enter**.
    The software installs automatically. Wait at least 5 minutes for the device to initialize.
14. Open a web browser and type the IP address of the device to start the Web UI Setup Wizard.
15. For example, `https://10.0.0.1`.
16. On the Login page, type the default user ID **admin**, and the default password **admin**.
17. Follow the instructions on the screen and complete the Wizard.
18. Make sure you update the feature key during the Wizard.

Restore the Configuration

1. Select **Administration > Backup/Restore > Backup and Restore**.
2. Select your restore method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
3. Select which information to restore. 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 **Restore now**.
   The XCS device reboots when the restore is complete.

To Install the Software Upgrade 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 to **Primary** mode.
4. Install the update on the **Secondary**, and then restart the device.
5. Change the run mode of the **Secondary** system to **Secondary** mode.
6. Install the update on any **Client** devices, and then restart the device.
7. Change the run mode of the **Client** device to **Client** mode.

Known Issues and Limitations

Known issues for XCS 10.2 including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To see known issues for a specific release, from the Product & Version filters you can expand the XCS version list and select the check box for v10.2.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at https://www.watchguard.com/wgrd-support/overview. 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