Fireware XTM v11.8.3 CSP 3 Release Notes

Supported Devices	Firebox T10, XTM 25/26 XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 1050, XTM 2050, XTMv, WatchGuard AP
Fireware XTM OS Build	451065
WatchGuard System Manager Build	N/A
Revision Date	June 10, 2014

Software Available for Download

To download software for this CSP release, go to:

ftp.watchguard.com/11.8.3_CSP/CSP3/
Username: XTM_CSP
Password: S0NofTr1ton

WatchGuard System Manager v11.8.3 or higher is needed to manage a device running Fireware XTM v11.8.3 CSP 3. Fireware XTM OS v11.8.3 CSP releases are cumulative. A description of available software files is included below the *Resolved Issues* sections.

11.8.3 CSP 3 contains an updated SSLVPN client with version 11.9.1

Resolved Issues in Update 1 (Build 446065)

NOTE: Update 1 included CSP 1

- This release includes an update to the OpenSSL libraries used in Fireware XTM v11.8.3 in response to the reported "Heartbleed" vulnerability (CVE-2014-0160). *[80014]*
- Proxies have been updated to recognize TLS v1.2 so that HTTPS traffic is now correctly blocked through the TCP-UDP proxy. *[78328]*
- Google HTTPS web sites now load correctly through the HTTPS proxy with DPI enabled when there is no response from the OCSP check. *[76194]*
- This release resolves an issue that caused Path MTU for BOVPN traffic to work incorrectly in Fireware XTM v11.8 releases. *[78942, 78829]*
- The maximum number of BOVPN routes per tunnel has been increased from 128 to 256. *[79208]*
- An issue has been resolved that caused RDP/Citrix user authentication to stop working after an undetermined time. *[77669]*

- A crash that resulted in this log message “Kernel Panic EIP is at e1000e_free_rx_resources+0xfc0/0x14ec [e1000e]” has been resolved. *[78854]*
- You can now complete the FTP-proxy "LIST" command when going through a tagged VLAN. *[78441]*
- This release adds USB modem support for Sierra Wireless, AT&T Mobile Hotspot Elevate 4G. *[78363]*
- HTTPS-Proxy traffic, when DPI is enabled, no longer fails when browsing to some web sites. *[77846]*
- A crashing problem that caused the log message “BUG: sleeping function called from invalid context EIP is at nl_pid_hash_rehash+0x7c/0xd3” has been resolved. *[78216]*
- Several kernel crashes have been resolved in this release. *[78798, 78799, 78454]*
- A memory leak triggered by continuous configuration changes using the CLI has been resolved. *[75734, 60142]*
- This release resolves an issue that prevented successful configuration saves after an upgrade to v11.8.1 because of invalid dynamic routing configuration settings. *[78734]*
- This release resolves an issue that prevented successful configuration saves to an XTM 1050 when the configuration contained over 600 firewall policies. *[78806]*
- The tracking of authenticated user names in the traffic log messages has been improved to allow for more accurate reporting. *[76581, 79774]*
- You can now use more than 21 characters in the WatchGuard Mobile SSLVPN client Server field. *[79333]*
- This release resolves an issue that caused the BOVPN Phase 1 SA to be missing during renegotiation with 3rd party IPSec devices. *[79260]*

Resolved Issues in CSP 2 (Build 449509)

- *[BUG78665, BUG78819]* This release resolves several proxy process crashes.
- *[BUG79235, RFE75725]* This release resolves several issues that occurred when using inbound HTTPS content inspection.
- *[BUG80328,BUG79733]* The SMTP proxy, when used with TLS, no longer causes excessive CPU use.
- *[BUG77987, BUG78807, BUG79043]* This release resolves several issues in which HTTPS web sites did not load correctly when using HTTPS content inspection.
- *[BUG77969]* SSLVPN connections using WatchGuard’s SSLVPN client or OpenVPN client are no longer blocked by the HTTPS proxy.
- *[BUG78793]* HTTPS sessions made from browsers Internet Explorer 10+ on Windows 8 will now establish more quickly when using an HTTPS proxy.
- *[BUG79643]* A memory leak has been resolved that occurred when large files were transferred through the FTP proxy.
- *[BUG80403]* Feature keys with more than 1024 characters are now supported.

- *[RFE72721]* If you use Active Directory (AD) authentication for Terminal Services users, a mismatch in capitalization (case) between the domain name configured in Setup > Authentication > Servers and your actual AD server no longer causes a failure to apply policies correctly to the users.
- *[BUG77944, BUG77935]* This release updates the ECMP algorithm used for Multi-Wan routing table mode to improve WAN load balancing performance.
- *[BUG79010]* A device configured in drop-In mode now correctly responds to an ARP request sent to a unicast address.
- *[BUG79832]* This release resolves a kernel crash.

Resolved Issues in CSP 3 (Build 451065)

- This release contains patches to the OpenSSL version used in the appliance and the SSLVPN client. The patch addresses the following OpenSSL advisories CVE-2014-0195, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470.
- *[BUG80315]* This release resolves an issue which caused traffic to fail when using the HTTP Proxy with WebBlocker. The traffic would fail with logs showing: *err webblocker[1903]: scan_wb: no profile found*
- *[BUG81008, BUG80885, BUG81037]* This release provides improvements to Application Control detection when not using HTTPS proxy with Content Inspection.
- *[BUG79962,BUG79311,BUG80385]* Several improvements were made to SIP ALG to fix occurrences of one way audio during VoIP calls.
- *[BUG79909]* This release solves a kernel crash triggered by a syn flood to the firewall.
- *[BUG79841]* A Kernel crash no longer occurs when the “maximum command line length” for the FTP proxy is exceeded and auto block is enabled.
- *[BUG77948]* This release resolves a proxy process crash when using IPS.

Available Files in this CSP Release

Software File	For Device Model	Information
WSM11_8_3.exe	All Firebox and XTM devices	WatchGuard System Management software
XTM_OS_XTM800_1500_2500_11_8_3.exe	XTM 800, 1500, or 2500 devices	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM2050_11_8_3.exe	XTM 2050 devices	Appliance software to install sysa-dl file on your computer

		to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM1050_11_8_3.exe	XTM 1050 devices	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM8_11_8_3.exe	XTM 8 Series devices	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM5_11_8_3.exe	XTM 5 Series devices	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM330_11_8_3.exe	XTM 330 devices	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM33_11_8_3.exe	XTM 33 devices	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_XTM2A6_11_8_3.exe	XTM 25 & 26 devices (including wireless)	Appliance software to install sysa-dl file on your computer to upload to your XTM device using Policy Manager or the XTM Web UI
XTM_OS_T10_11_8_3.exe	Firebox T10 devices	Appliance software to install sysa-dl file on your computer to upload to your Firebox using Policy Manager or the XTM Web UI
XTMv_11_8_3.ova	XTMv with VMware	File to do initial installation of XTMv for VMware
xtmv_11_8_3_vhd.zip	XTMv with Hyper-V	File to do initial installation of XTMv for Hyper-V
XTM_OS_XTMV_11_8_3.exe	XTMv, all editions	File to upgrade an existing XTMv installation. Applies to VMware and Hyper-V installations.