Fireware XTM v11.8.1 CSP3

Supported Devices

XTM 3, 5, 8, 800, 1500, and 2500 Series
XTM 25, XTM 26, XTM 1050, XTM 2050
XTMv, WatchGuard AP

Fireware XTM OS Build # 441333

WSM v11.8.1 or higher is needed to manage a device running Fireware XTM 11.8.1 CSP. 11.8.1 CSP releases are cumulative.

Software Available at:

ftp.watchguard.com/11.8.1_CSP/CSP3/

Username: XTM_CSP

Password: S0NofTr1ton

Resolved Issues:

CSP1 (Build # 440610)

[BUG78331] Resolved issue that caused a FireCluster member to remain in the IDLE state if the member loses the Master election process.

[BUG76986] Dynamic Routing continues to work after unplugging an External Interface when using Multi-WAN with failover from Dynamic Route to BOVPN.

[BUG78239] Resolved issue that prevented Proxy traffic from passing when using bridge mode and tagged VLAN.

[BUG76952] Resolved issue that caused the virtual IP assigned to an IPSec Mobile User to not be released after the Mobile User disconnected.

[BUG76405] Resolved occurrence of Network Card interface hang under high load with very small packets.

[BUG78057] LDAP user authentication with groupMembership attribute no longer fails in XTM 11.8

[BUG70152] Resolved issue causing a short traffic disruption for established SSLVPN connections, when another SSLVPN user connects or disconnects from the Firewall.

[BUG77769, BUG78447, BUG78639] Resolved issues causing some browsers to not properly verify certificate chain for some HTTPS websites when using the HTTPS Proxy with DPI enabled.

CSP2 (Build # 440969)

Fixed issue in 11.8.1 CSP1 which caused WebBlocker lookups to fail when using Websense due to invalid Websense server URL in the CSP1 release.

CSP3 (Build # 441333)

[BUG78692] Resolved IKED process crash.

[BUG78749] This release includes a fix for a cross-site scripting vulnerability that affects one of the parameters used in the Fireware XTM Web UI. To exploit this vulnerability, an attacker would first have to trick an XTM administrator into clicking a specially-crafted link, and then entering their XTM management credentials. However, if the attack succeeds the attacker can do everything in the XTM management UI that the administrator could (and may gain elevated privilege to that administrator's browser). Though the required user interaction lessens the severity of this vulnerability, we recommend you apply the update. You can also mitigate this issue by making sure not to expose your management interface externally, and by avoiding clicking on unsolicited links. VU#233990

Description of v11.8.1 CSP files available for download:

XTM_OS_XTM800_1500_2500_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the XTM 800, 1500,2500 Series Firewalls using policy manager or the WebUI

XTM_OS_XTM2050_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the 2050 using policy manager or the WebUI

XTM_OS_XTM1050_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the 1050 using policy manager or the WebUI

XTM_OS_XTM8_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the XTM 8-series using policy manager or the WebUI

XTM_OS_XTM5_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the XTM 5-series using policy manager or the WebUI

XTM_OS_XTM330_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the XTM 330 using policy manager or the WebUI

XTM_OS_XTM330_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the XTM 33 using policy manager or the WebUI

XTM_OS_XTM2A6_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to the XTM25 and XTM26 using policy manager or the WebUI

XTMv_11_8_1.ova -- File to do initial installation of XTMv for VMware

xtmv_11_8_1_vhd.zip - File to do initial installation for Hyper-V

XTM_OS_XTMV_11_8_1.exe -- File to upgrade an existing XTMv installation. Applies to VMware and Hyper-V installations