Fireware XTM v11.8.1 CSP4

Introduction

Supported Devices

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

Build Information & File Location

Fireware XTM OS Build # 441999

WatchGuard System Manager Build # 442038

WSM v11.8.1 or higher is needed to manage a device running Fireware XTM v11.8.1 CSP 4. XTM OS v11.8.1 CSP releases are cumulative.

Software Available at:

ftp.watchguard.com/11.8.1_CSP/CSP4/

Username: XTM_CSP

Password: S0NofTr1ton

Resolved Issues

CSP1 (Build # 440610)

[BUG78331] This CSP resolves an issue that caused a FireCluster member to remain in the IDLE state when the member loses the Master election process.

[BUG76986] Dynamic Routing continues to work after an external interface is unplugged, in a network configured for Multi-WAN with failover from Dynamic Route to BOVPN.

[BUG78239] This release resolves an issue that prevented proxy traffic from passing through an XTM device configured in bridge mode with a tagged VLAN.

[BUG76952] Virtual IP address assigned to an IPSec Mobile User are now correctly released after a mobile user disconnects.

[BUG76405] A problem that caused a network card interface to hang under high load with very small packets has been resolved.

[BUG78057] LDAP user authentication with groupMembership attribute no longer fails.

[BUG70152] A short traffic disruption for established Mobile VPN with SSL connections no longer occurs when another SSLVPN user connects or disconnects from the firewall.

[BUG77769, BUG78447, BUG78639] This release resolves several issues that caused some browsers to incorrectly verify certificate chain for some HTTPS websites when using the HTTPS Proxy with DPI enabled.

CSP2 (Build # 440969)

This CSP resolves in issued introduced in XTM v11.8.1 CSP1 that caused WebBlocker lookups to fail when using Websense because of an invalid Websense server URL.

CSP3 (Build # 441333)

[BUG78692] An IKED process crash has been resolved.

[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

CSP4

Appliance Build # 441999

[BUG78152] An issue that prevented some HTTPS websites from correctly loading in the Chrome browser when HTTPS Proxy with DPI is enabled has been resolved.

[BUG78880] This release resolves an issued that prevented a managed device from consistently contacting the Management Server when the device lease expired.

[BUG77230] HostWatch no longer shows *Unknown* for the source when it displays proxy connections.

[BUG78507] The Sierra 320U modem is now supported on these XTM device models: XTM 25/26, XTM 33, XTM 330.

[BUG78831] The wrong source IP address is no longer used for DHCP relay packets sent though a VLAN interface and a Branch Office VPN tunnel.

WSM Build # 442038

[BUG78766] This release resolves an issue that prevented a template save from Management Server v11.8.1 to a device configured with Deep Packet Inspection running a release prior to v11.8.1. The configuration save from the Management Server failed and generated this log message in the appliance log file: dvcpcd Error line 13025:Element 'allow-non-ssl': This element is not expected. Expected is one of (bypass-list, transaction, self_signed, filter, domain-name). Debug

[BUG78643, BUG78483] An Apache server crash on the WatchGuard Management Server has been resolved in this release.

[BUG76648] This release resolves an issue that prevented a template save from Management Server v11.8.1 when the managed device uses a third-party web server certificate.

[RFE78041] The managed device folder on the Management Server now shows the model number of the device, the software version in use, the management mode (Full or Basic) and what management groups the device belongs to.

[BUG78851] The WSM Report Server PDF report now displays Japanese fonts correctly.

Description of XTM 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 XTM 800, 1500, 2500 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM2050_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to 2050 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM1050_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to 1050 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM8_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to XTM 8 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM5_11_8_1.exe -- appliance firmware to install sysa-dl file on your PC to upload to XTM 5 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM330_11_8_1.exe   -- appliance firmware to install sysa-dl file on your PC to upload to XTM 330 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM330_11_8_1.exe   -- appliance firmware to install sysa-dl file on your PC to upload to XTM 33 Series devices using Policy Manage or the XTM Web UI

XTM_OS_XTM2A6_11_8_1.exe   -- appliance firmware to install sysa-dl file on your PC to upload to XTM25 and XTM26 Series devices using Policy Manage or the XTM Web UI

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 of XTMv for Hyper-V

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