WSA Upgrade Failure from SMA Due to Invalid SSL Configuration

Contents

Issue

When attempting to upgrade a WSA (Web Security Appliance) from SMA (Security Management Appliance), the upgrade process fails with the error message "Update failed Failed to upgrade (Reason: Invalid SSL configuration)." The upgrade is successful when performed directly from the WSA web interface, but consistently fails when initiated from the SMA. Attempts to resolve the issue by generating a new self-signed certificate and changing the default authentication certificate were unsuccessful.

Environment

- Cisco Web Security Appliance (WSA)
- Software Version: 15.2.2-009 (MD)
- Cisco Security Management Appliance (SMA)
- Target Upgrade Version: AsyncOS 15.5
- DNS functionality verified and working correctly

Resolution

The resolution involves disabling legacy TLS versions (TLSv1.0 and TLSv1.1) on the WSA appliance to meet the upgrade prerequisites for AsyncOS 15.5.

Step 1: Identify the Root Cause

The upgrade failure is caused by a change in AsyncOS 15.5 behavior where TLSv1.0 and TLSv1.1 are no

longer supported in any SSL configuration other than the proxy configuration. The upgrade process requires TLSv1.2 or later for non-proxy SSL configurations.

Step 2: Disable Legacy TLS Versions

Disable TLSv1.0 and TLSv1.1 on the WSA appliance through the configuration interface. This change satisfies the upgrade prerequisite and allows the upgrade process to continue.

Step 3: Verify External Service Compatibility

Ensure external services such as LDAP support TLSv1.2 or later versions. As long as these services are compatible with TLSv1.2 and later, the upgrade does not break communication with external systems.

Step 4: Proceed with Upgrade

After disabling the legacy TLS versions, retry the upgrade process from the SMA. The upgrade can now proceed without the "Invalid SSL configuration" error.

Step 5: Monitor and Validate

Monitor the upgrade process to ensure successful completion and validate all dependent services continue to function properly with TLSv1.2 after the upgrade.

Cause

The upgrade failure is caused by a behavioral change introduced in AsyncOS 15.5.0-566 where TLSv1.0 and TLSv1.1 are no longer supported in any SSL configuration other than the proxy configuration. This creates an upgrade prerequisite that requires changing the TLS version to TLSv1.2 or later before upgrading AsyncOS. The SMA upgrade process performs pre-upgrade validation checks that detect this incompatibility and prevent the upgrade from proceeding.

Related Content

- AsyncOS 15.5 Release Notes
- Cisco Technical Support & Downloads