Update DNS Umbrella Certificate to Work in October 2024

Contents

Introduction

Background Information

Defect Information

Fixed Released

- CCO Releases

Remediation Matrix

- 1. Cisco Devices Running Cisco IOS XE Software Release 17.5.x or Earlier in Controller Mode
  - Automated
  - Manual
- 2. Cisco Devices Running Cisco IOS XE Software Release 17.6.x to 17.8.x in Controller Mode
  - Automated
  - Manual
- 3. Cisco Devices Running Cisco IOS XE Software Release 17.9.5a in Controller Mode
- 4. Cisco Devices Running Cisco IOS XE Software Release 17.9.6 in Controller Mode
- 5. Cisco Devices That Are Cisco IOS XE Software Release 17.12.3a in Controller Mode
- 6. Cisco Devices Running Cisco IOS XE Software Release 17.12.4 in Controller Mode

Introduction

This document describes how to resolve the DNS Umbrella issue where SD-WAN routers use the expired certificate instead of the new one.

Background Information

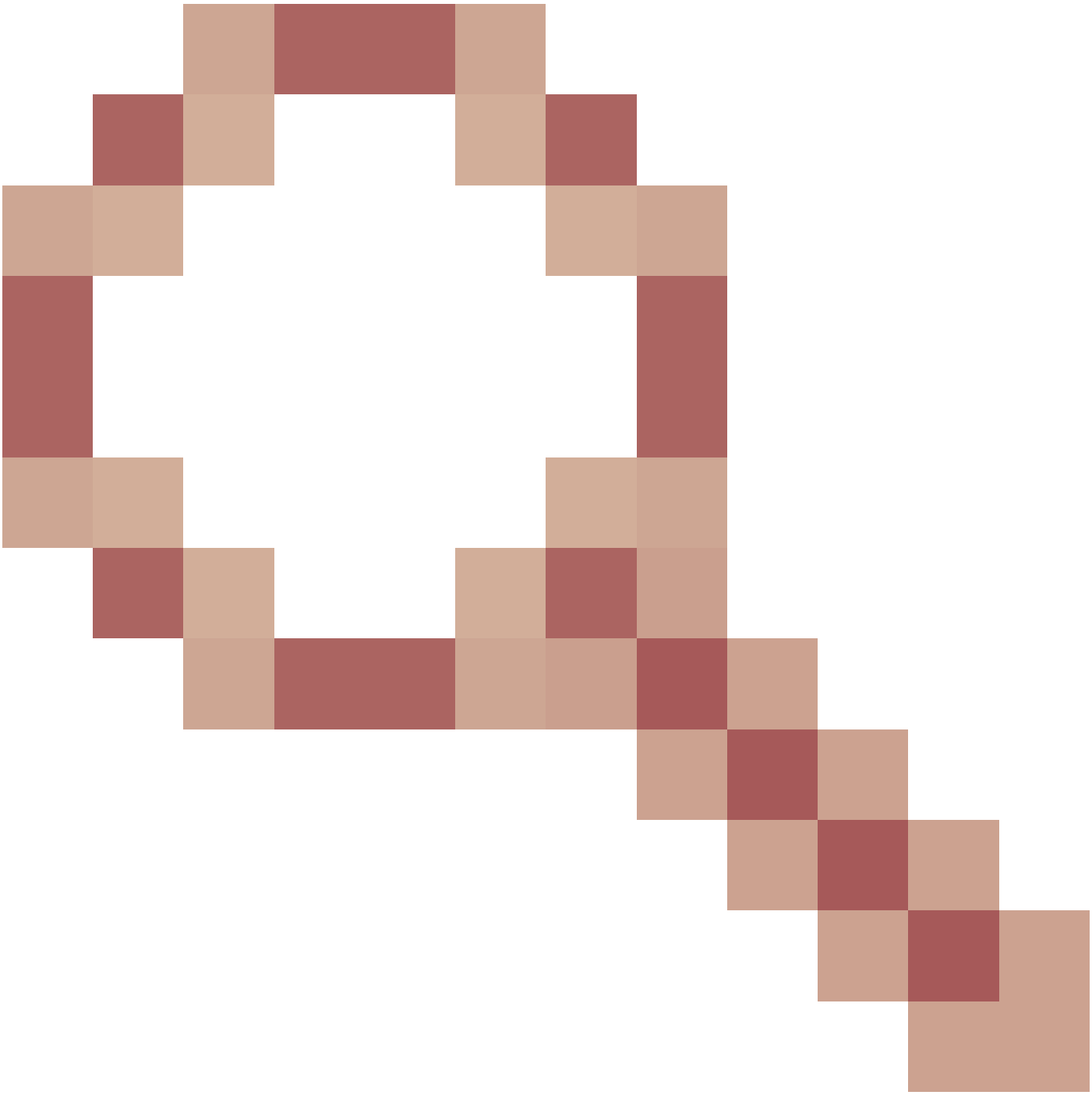
The digital certificate that is used by Cisco Catalyst SD-WAN Routers to register using the API Key/Secret authentication method with Cisco Umbrella DNS expired on September 30, 2024. Cisco SD-WAN Routers with the expired certificate will fail to register with the Cisco Umbrella DNS service. This issue does not apply to the Token based authentication for the Umbrella DNS registration.

Refer to the Cisco Umbrella DNS certificate expiry on September 30, 2024, in Field Notice FN74166 for more details.

Affected SD-WAN devices with expired umbrella root CA certificate cannot establish secure connections with the Cisco Umbrella DNS for device registration. As the device is not registered with Umbrella DNS Service, end-user DNS requests are not redirected to the Umbrella domain server by SD-WAN edge for DNS Security policy enforcement. The DNS request from the end-users behind the SD-WAN edge will not be dropped and is serviced by the DNS domain server configured on the end-user devices.

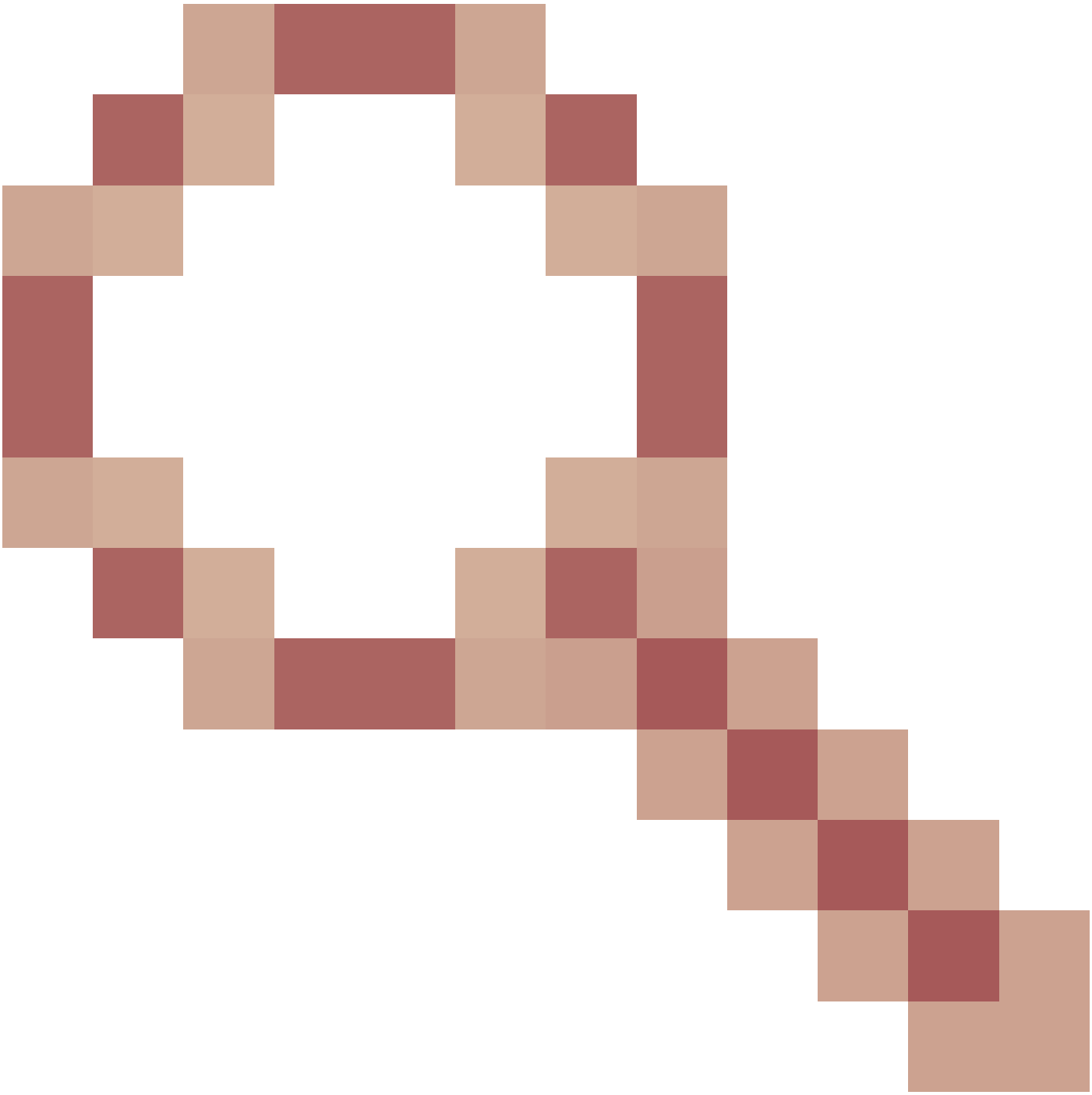
Defect Information

The certificate was updated as part of Cisco bug ID CSCwi43360



: Cert expiry on Sept 2024 for DNS Security registration to Umbrella cloud. (fixed in 17.9.6, 17.12.4,17.15.1a)

Even with the certificate being updated the SSL handshake fails to establish, which is addressed as part of Cisco bug ID CSCwm73365



: SSL handshake fails despite umbrella_root_ca.ca with the latest certificate being present on the device. (fixed in 17.6.8a)

Fixed Released

CCO Releases

Release	17.6.8a

ENGINEERING SPECIAL Releases

Release	17.09.05a.0.51
Release	17.12.04.0.31

Remediation Matrix

Releases	Cisco Recommended Remediation Steps
17.3.x/17.4.x/17.5.x	Follow the steps in section 1. Cisco Devices Running Cisco IOS XE Software Release 17.5.x or Earlier in Controller Mode
17.6.1-17.6.7, 17.7.x, 17.8.x	Follow the steps in section 2. Cisco Devices Running Cisco IOS XE Software Release 17.6.x to 17.8.x in Controller Mode
17.6.8a	The Umbrella DNS Cert expiry issue is fixed in this release.
17.9.1 – 17.9.4, 17.10.x, 17.11.x, 17.12.1-17.12.2, 17.13.x, 17.14.x, 17.15.1a	Use Umbrella DNS Cert Script for automated certificate copy to the Edge devices. Refer to the readme file on the GIT for the steps to use for running the script.
17.9.5a	Follow the steps in section 3
17.9.6	Follow the steps in section 4
17.12.3a	Follow the steps in section 5
17.12.4	Follow the steps in Section 6

1. Cisco Devices Running Cisco IOS XE Software Release 17.5.x or Earlier in Controller Mode

Use the remediation options to install the new Umbrella RootCA certificate.

Automated

1. For SD-WAN Manager 20.9.1 or higher use the Umbrella DNS Cert script for automated certificate copy to the edge devices from vManage.
2. Umbrela DNS Cert Script
3. Refer to the readme file on the GIT for detailed steps to use the script.
4. After the RootCA certificate is copied to the device, reload the router to complete the installation process.

Manual

1. Download the new unexpired certificate from the New Umbrella Certificate website and place it on a device that has access to the affected router(s) in the SD-WAN overlay.
2. Enter the Linux scp command or similar mechanism to perform a secure file copy from the download device onto each affected router.

   For example:

   scp ./isrgrootx1.pem <Username>@<EdgeIP>:trustidrootx3_ca.ca

   Substitute <Username> with an admin user and <EdgeIP> with the IP address of the affected router.

3. After the RootCA certificate is copied to the device, reload the router to complete the installation process.

2. Cisco Devices Running Cisco IOS XE Software Release 17.6.x to 17.8.x in Controller Mode

Use the remediation options to install the new Umbrella RootCA certificate.

Automated

1. For SD-WAN Manager 20.9.1 or higher use the Umbrella DNS Cert script for automated certificate copy to the edge devices from vManage.
2. Umbrella DNS Cert Script
3. Refer to the readme file on the GIT for detailed steps to use the script.
4. After the RootCA certificate is copied to the device, reload the router to complete the installation process.

Manual

1. Download the new unexpired certificate from the New Umbrella Certificate website and place it on a device that has access to the affected router(s) in the SD-WAN overlay.
2. Enter the Linux **scp** command or similar mechanism to perform a secure file copy from the download device onto each affected router.

   For example:

   scp ./isrgrootx1.pem admin@<*EdgeIP*>:trustidrootx3_ca_092024.ca

   Substitute <*EdgeIP*> with the IP address of the affected router.

3. After the RootCA certificate is copied to the device, reload the router to complete the installation process

3. Cisco Devices Running Cisco IOS XE Software Release 17.9.5a in Controller Mode

Use the remediation options to install the new Umbrella RootCA certificate as explained in this section, for most platforms there is a HOT SMU available with the fix. You also have the option to run the Script mentioned to install the new Umbrella RootCA certificate.

1. The HOT SMU applies to these platforms – *"Hitless/Recommended SMU, SSL handshake fails despite umbrella_root_ca.ca with latest certificate being present on the device"* :

   4431 Integrated Services Router
   4451-X Integrated Services Router

   ASR 1001-X Router
   Virtual Routers
   4331 Integrated Services Router
   4221 Integrated Services Router
   4351 Integrated Services Router
   Catalyst 8500L Edge Platform
   ASR 1001-HX Router
   4321 Integrated Services Router

   Catalyst 8500 Edge Platform

   4461 Integrated Services Router

2. Alternative to SMU, run the script Umbrella DNS Cert Script Refer to the readme file on the GIT for detailed steps to use the script.

Script only option for:
ASR1002-X Router

Catalyst 8300 Edge Platform

ISR 1000 Series running Cisco IOS XE SD-WAN

4. Cisco Devices Running Cisco IOS XE Software Release 17.9.6 in Controller Mode

1. The HOT SMU applies to these platforms – *"Hitless/Recommended SMU, SSL handshake fails despite umbrella_root_ca.ca with latest certificate being present on the device*":

   4221 Integrated Services Router
   4321 Integrated Services Router
   4451-X Integrated Services Router
   Catalyst 8500 Edge Platform
   4431 Integrated Services Router
   Virtual Routers
   4461 Integrated Services Router
   4331 Integrated Services Router
   4351 Integrated Services Router
   ASR 1001-HX Router
   ASR 1001-X Router
   Catalyst 8500L Edge Platform

   Catalyst 1101 Rugged Router

   Catalyst IR1831 Rugged Router
   Catalyst IR1821 Rugged Router
   Catalyst IR1833 Rugged Router
   Catalyst IR1835 Rugged Router

3. Alternative to SMU, run the script Umbrella DNS Cert Script Refer to the readme file on the GIT for

detailed steps to use the script.

Script only option for:

ASR1002-X Router

Catalyst 8300 Edge Platform

ISR 1000 Series running Cisco IOS XE SD-WAN

5. Cisco Devices That Are Cisco IOS XE Software Release 17.12.3a in Controller Mode

1. The HOT SMU applies to these platforms – "*Hitless/Recommended SMU, SSL handshake fails despite umbrella_root_ca.ca with latest certificate being present on the device*":

   4221 Integrated Services Router
   Catalyst 8300 Edge Platform
   4331 Integrated Services Router
   4461 Integrated Services Router
   1100 Integrated Services Router
   4351 Integrated Services Router
   4321 Integrated Services Router
   4431 Integrated Services Router
   Virtual Routers
   4451-X Integrated Services Router

   Catalyst 8500L Edge Platform
   Catalyst 8500 Edge Platform
   ASR 1001-HX Router

2. Alternative to SMU, run the script Umbrella DNS Cert Script

Refer to the readme file on the GIT for detailed steps to use the script.

6. Cisco Devices Running Cisco IOS XE Software Release 17.12.4 in Controller Mode

1. The HOT SMU applies to these platforms – "*Hitless/Recommended SMU, SSL handshake fails despite umbrella_root_ca.ca with latest certificate being present on the device*":

   Catalyst 8500 Edge Platform
   ASR 1001-HX Router
   4331 Integrated Services Router
   4321 Integrated Services Router
   4221 Integrated Services Router
   Virtual Routers
   4351 Integrated Services Router
   4451-X Integrated Services Router
   4461 Integrated Services Router
   Catalyst 8300 Edge Platform
   ASR 1002-HX Router
   4431 Integrated Services Router

   1100 Integrated Services Router

Catalyst 8500L Edge Platform

Catalyst IR1833 Rugged Router
Catalyst IR1835 Rugged Router
Catalyst IR1831 Rugged Router
Catalyst IR1821 Rugged Router

2. The alternative to SMU is to run the script Umbrella DNS Cert Script Refer to the readme file on the GIT for detailed steps to use the script.

⚠ **Caution**: Umbrella DNS Registrations from the Devices continue to work as long as there is no reboot of the device or no new registrations.

⚠ **Caution**: If the umbrella configuration is removed and re-applied, this triggers the re-registration of the umbrella DNS. As long as this process is not followed, the umbrella DNS functions properly.
