

Sicherer Client ZTNA DNS-Auflösung und Verbindungsverlust nach MacOS-Ruhemodus

Inhalt

Problem

Bei Cisco SecureClient ZTNA an macOS-Endgeräten treten nach der Wiederherstellung des Energiesparmodus oder des Ruhezustands des Systems ein DNS-Auflösungsfehler und ein ZTNA-Verbindungsverlust auf. Dieses Problem betrifft sowohl ZTNA IA (Identity Access) als auch ZTNA PA (Private Access) Funktionalität. Obwohl die grundlegende IP-Verbindung weiterhin funktioniert (ICMP führt einen Ping an externe IP-Adressen wie 8.8.8.8 und 208.67.222.222 erfolgreich durch), schlägt die DNS-Namensauflösung vollständig fehl, wodurch der Zugriff auf Internetressourcen und private Ressourcen, die über ZTNA konfiguriert wurden, verhindert wird.

Zu den beobachteten spezifischen Symptomen gehören:

- DNS-Lookups schlagen mit nslookup-Befehlen fehl (wie nslookup von www.cisco.com über 8.8.8.8 und 208.67.222.222 funktioniert nicht).
- ZTNA IA- und ZTNA PA-Verbindungen sind nicht mehr verfügbar.
- Das Problem tritt konsistent nach dem Ruhezustand und dem Aktivierungszyklus des Endgeräts auf.
- Das Problem kann auch zufällig auftreten, wenn das Gerät aktiv genutzt wird.
- Wenn Sie den ZTNA-Prozess abbrechen, wird der Vorgang sofort neu gestartet. Das Verbindungsproblem besteht jedoch in der Regel weiterhin.
- Nur ein vollständiger Systemneustart stellt die vollständige DNS-Auflösung und ZTNA-Konnektivität wieder her.

Umwelt

- Betriebssystem: macOS (Version 26.3 dokumentiert für den Fall)

- Cisco SecureClient: Version 5.1.14.x (betroffene Versionen vor 5.1.16)
- ZTNA-Modul: Aktiv mit IA- (Identity Access) und PA-Konfigurationen
- Netzwerküberwachung: Umfasst Sicherheitslösungen von Drittanbietern wie Sentinel One
- Zusätzliche Sicherheitssoftware: Kann Cisco Secure Endpoint enthalten
- DNS-Server: Externe DNS-Server (8.8.8.8, 208.67.222.222), auf die über ICMP zugegriffen werden kann, aber DNS-Auflösung schlägt fehl
- UMB-Modul: Nicht verwendet

Auflösung

Das Problem wurde durch einen von Cisco Engineering bereitgestellten Software-Fix behoben. Der Auflösungsprozess umfasste die in den nächsten Abschnitten beschriebenen Schritte.

Schritt 1: Problemerkennung und Fehlerverfolgung

Cisco Engineering hat dies als bekannten Fehler identifiziert und unter der Cisco Bug-ID CSCwt24392 mit der Beschreibung "macOS: DNS funktioniert nicht mehr mit ZTA SIA-all und NVM aktiv".

Phase 2: Diagnosedatenerfassung

Diese Diagnoseinformationen wurden zur Unterstützung der technischen Analyse gesammelt:

- DART (Diagnostic and Reporting Tool)-Pakete von betroffenen Endgeräten
- Paketerfassungsdateien (ZTNA Issue1.pcapng).
- Screenshots zum Nachweis eines Verbindungsfehlers.
- Screenshots zur Reproduktion des Problems
- Prozessinteraktionsprotokolle, die das Verhalten von com.cisco.secureclient.zta.app.service und Systemerweiterungen anzeigen.

Schritt 3: Engineering Fix-Entwicklung

Cisco Engineering hat einen zielgerichteten Fix für CSCwt24392 entwickelt und in SecureClient Version 5.1.16 integriert. Der Fix behandelt speziell den DNS-Auflösungsfehler, der auftritt, wenn ZTA SIA-all und NVM nach dem Standby-/Ruhemodus auf macOS-Systemen aktiv sind.

Schritt 4: Installation von Software-Updates

Installieren Sie Cisco SecureClient Version 5.1.16 oder höher auf betroffenen macOS-Endgeräten. Diese Version enthält die Behebung von DNS-Auflösungs- und ZTA-Verbindungsproblemen.

Schritt 5: Validierungstests

Führen Sie nach der Installation von SecureClient 5.1.16 die folgenden Validierungsschritte durch:

- 1.- Lassen Sie den macOS-Endpunkt in den Standby- oder Ruhemodus wechseln.
- 2.- Wecken Sie das System aus dem Schlaf oder Winterschlaf.
- 3.- Testen der DNS-Auflösung mit nslookup-Befehlen
- 4.- Überprüfen der ZTNA IA- und ZTNA PA-Verbindung zu konfigurierten Ressourcen
- 5.- Bestätigen Sie, dass sowohl der Internetzugang als auch der Zugriff auf private Ressourcen ordnungsgemäß funktionieren, ohne dass ein Systemneustart erforderlich ist.

Problemumgehung für frühere Versionen

In Umgebungen, in denen ein sofortiges Upgrade auf SecureClient 5.1.16 nicht möglich ist, kann diese temporäre Problemumgehung verwendet werden:

- Führen Sie nach jedem Ruhemodus-/Ruhemodus einen vollständigen Systemneustart

durch, um die DNS-Auflösung und die ZTNA-Konnektivität wiederherzustellen.

- Erwägen Sie, sich vorübergehend von ZTNA abzumelden, wenn sich das Problem mit dem Schlaf-/Ruhemodus erheblich auf die Produktivität auswirkt (beachten Sie, dass dadurch der ZTNA-Schutz aufgehoben wird).

Ursache

Ursache dieses Problems ist ein Softwarefehler in Cisco SecureClient-Versionen vor 5.1.16, der als Cisco Bug-ID CSCwt24392 verfolgt wird. Der Fehler tritt auf, wenn die Komponenten ZTA (Zero Trust Access) SIA-all (Secure Internet Access) und NVM (Network Visibility Module) auf macOS-Systemen aktiv sind. Während des Standby-, Ruhemodus- und Aktivierungszyklus können diese Komponenten die DNS-Auflösungsfunktion nicht ordnungsgemäß wiederherstellen und gleichzeitig die grundlegende IP-Verbindung beibehalten. Dadurch wird ein Zustand erzeugt, in dem der ICMP-Datenverkehr (Ping) normal funktioniert, die DNS-Abfragen jedoch fehlschlagen. Dadurch wird der Zugriff auf Internetressourcen und private ZTNA-geschützte Ressourcen effektiv blockiert. Das Problem besteht in einer unzulässigen Interaktion zwischen dem com.cisco.secureclient.zta.app.service-Prozess und dem Systemerweiterungsprozess bei Übergängen des Systemstatus.

Verwandte Inhalte

- Cisco Bug-ID CSCwt24392 - macOS: DNS funktioniert nicht mehr mit ZTA SIA-all und NVM aktiv
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.