Beveiligde ZTNA-clientoplossing en verlies van connectiviteit na overwintering van macOS

Inhoud

uitgifte

Cisco SecureClient ZTNA op macOS-eindpunten ervaart een storing in de DNS-resolutie en verlies van ZTA-connectiviteit nadat het systeem uit de slaap- of slaapstand is gehaald. Dit probleem is van invloed op zowel ZTNA IA (Identity Access) als ZTNA PA (Private Access). Hoewel de basis-IP-connectiviteit functioneel blijft (ICMP-ping naar externe IP-adressen zoals 8.8.8.8 en 208.67.222.222 werkt met succes), mislukt de DNS-naamresolutie volledig, waardoor toegang tot zowel internetbronnen als privébronnen die zijn geconfigureerd via ZTNA wordt voorkomen.

De specifieke symptomen die zijn waargenomen zijn:

- DNS-opzoeken mislukt met behulp van nslookup-opdrachten (zoals nslookup van www.cisco.com via 8.8.8.8 en 208.67.222.222 werkt niet).
- ZTNA IA- en ZTNA PA-verbindingen zijn niet meer beschikbaar.
- Probleem treedt consequent op na de eindpuntsluimerstand en wekcycli.
- Problemen kunnen ook willekeurig optreden terwijl het apparaat actief in gebruik is.
- Het doden van het ZTNA-proces resulteert in een onmiddellijke herstart, maar het connectiviteitsprobleem blijft meestal bestaan.
- Alleen bij een volledige systeemherstart worden de volledige DNS-resolutie en ZTNA-connectiviteit hersteld.

milieu

- Besturingssysteem: macOS (versie 26.3 gedocumenteerd in case)

- Cisco SecureClient: versie 5.1.14.x (betrokken versies vóór 5.1.16)
- ZTNA-module: actief met configuraties voor Identity Access (IA) en Private Access (PA)
- Netwerkbewaking: kan beveiligingsoplossingen van derden zoals Sentinel One omvatten
- Extra beveiligingssoftware: kan Cisco Secure Endpoint bevatten
- DNS-servers: externe DNS-servers (8.8.8.8, 208.67.222.222) die toegankelijk zijn via ICMP, maar de DNS-resolutie mislukt
- UMB-module: niet in gebruik

resolutie

Het probleem werd opgelost door een softwarefixatie die door Cisco Engineering werd geleverd. Het afwikkelingsproces omvatte de stappen die in de volgende secties worden beschreven.

Stap 1: Identificatie van problemen en tracering van fouten

Cisco Engineering identificeerde dit als een bekend defect en logde het onder Cisco bug ID CSCwt24392 met de beschrijving "macOS: DNS stopt met werken met ZTA SIA-all en NVM actief".

Stap 2: Diagnostische gegevensverzameling

Deze diagnostische informatie werd verzameld om de technische analyse te ondersteunen:

- DART (Diagnostic and Reporting Tool) bundelt van de betrokken eindpunten.
- Packet capture-bestanden (ZTNA Issue1.pcapng).
- Schermafbeeldingen die de connectiviteitsstoring aantonen.
- Schermopnamen die het reproductieprobleem weergeven.
- Procesinteractielogboeken met het gedrag van com.cisco.secureclient.zta.app.service en systeemextensieprocessen.

Stap 3: Engineering Fix-ontwikkeling

Cisco Engineering ontwikkelde een gerichte oplossing voor CSCwt24392 en nam deze op in SecureClient versie 5.1.16. De oplossing richt zich specifiek op de DNS-oplossingsfout die optreedt wanneer ZTA SIA-all en NVM actief zijn op macOS-systemen na slaap-/winterslaap.

Stap 4: Installatie van software-update

Installeer Cisco SecureClient versie 5.1.16 of hoger op de betreffende macOS-eindpunten. Deze versie bevat de oplossing voor de DNS-oplossing en ZTA-connectiviteitsproblemen.

Stap 5: Validatie testen

Voer na installatie van SecureClient 5.1.16 de volgende valideringsstappen uit:

1.- Laat het macOS-eindpunt in de slaap- of winterslaapstand komen.

2.- Wek het systeem uit de slaap of winterslaap.

3.- Test de DNS-resolutie met behulp van nslookup-opdrachten.

4.- Controleer de ZTNA IA- en ZTNA PA-connectiviteit op geconfigureerde bronnen.

5.- Bevestig dat zowel internettoegang als toegang tot privébronnen naar behoren werken zonder dat het systeem opnieuw moet worden opgestart.

Workaround voor eerdere versies

Voor omgevingen waarin een onmiddellijke upgrade naar SecureClient 5.1.16 niet mogelijk is, kan deze tijdelijke oplossing worden gebruikt:

- Voer na elke slaap-/winterslaap een volledige systeemherstart uit om de DNS-resolutie en

ZTNA-connectiviteit te herstellen.

- Overweeg tijdelijk uit te schrijven van ZTNA als het slaap- / winterslaapprobleem de productiviteit aanzienlijk beïnvloedt (merk op dat dit ZTNA-bescherming verwijdert).

Oorzaak

De hoofdoorzaak van dit probleem is een softwaredefect in Cisco SecureClient-versies vóór 5.1.16, specifiek bijgehouden als Cisco bug ID CSCwt24392. Het defect treedt op wanneer de componenten ZTA (Zero Trust Access) SIA-all (Secure Internet Access) en NVM (Network Visibility Module) actief zijn op macOS-systemen. Tijdens de slaap- of winterslaap- en waakcyclus slagen deze componenten er niet in om de DNS-resolutiefunctionaliteit correct te herstellen, terwijl de basis-IP-connectiviteit behouden blijft. Dit creëert een staat waarin ICMP-verkeer (ping) normaal functioneert, maar DNS-query's mislukken, waardoor de toegang tot internetbronnen en ZTNA-beveiligde privébronnen effectief wordt geblokkeerd. Het probleem betreft onjuiste interactie tussen het com.cisco.secureclient.zta.app.service-proces en het systeemuitbreidingsproces tijdens systeemstatusovergangen.

Gerelateerde inhoud

- Cisco Bug ID CSCwt24392 - macOS: DNS stopt met werken met ZTA SIA-all en NVM actief
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.