ZTNA-Client - Netzwerkabfangfehler

Inhalt

Problem

Benutzer mit Netzwerkabfangfehlern beim Zugriff auf private Ressourcen über Cisco Secure Access Zero Trust Access (ZTNA). Der Fehler verhindert, dass eine Verbindung zu privaten Ressourcen hergestellt werden kann, die in der Umgebung mit dem nicht vertrauenswürdigen Zugriff konfiguriert sind, was zu einem vollständigen Verlust des Zugriffs auf interne Anwendungen und Dienste führt.

Umwelt

- Technologie: Cisco Secure Access - ZTNA (Zero Trust Access)
- Software-Version: 5.1.14
- Produktfamilie: SECACS
- Fehlertyp: Netzwerk-Abfangfehler
- Auswirkungen: Kritisch - Vollständiger Verlust des Zugriffs auf private Ressourcen
- Zuletzt durchgeführte Änderungen: Keine gemeldet

Auflösung

Dies wird in den DART-Protokollen angezeigt:

++ Die folgenden Protokolle wurden gefunden:

E/ ZtnaKdfConfigurator.cpp:208 ZtnaKdfConfigurator::StartIntercept() IZtnaApi::SetParameters failed with error code=BadParameter

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] E/ ZtnaConfigEnforcer.cpp:444 ZtnaConfigEnforcer::applyActiveSteeringPolicy() fehlgeschlagen ZTNA-Abfangen starten/aktualisieren

2026-03-02 11:33:30.933701 csc_zta_agent[0x000020fc/config_enforcer, 0x00001994] I/ZnConfigEnforcer.cpp:145 ZnConfigEnforcer::reportInterceptorConnectivityChange() Reporting KDF-Erreichbarkeit: Konfiguration fehlgeschlagen

in der zwischengespeicherten Konfiguration von DART

Ein nachgestelltes Leerzeichen wird eingeführt - cisco.com - und verursacht das Problem.

- Nach weiteren Tests hat sich herausgestellt, dass die Auswahl der Option für die remote erreichbare Adresse für die private Ressourcenkonfiguration und das Feld für die remote

erreichbare Adresse unverändert ist oder dieselben Werte wie die intern erreichbare Adresse hat. Diese Einstellung deaktiviert sich beim Speichern.
- Es sieht jedoch so aus, als ob bei der Überprüfung des Felds für die remote erreichbare Adresse ein zusätzlicher Leerraum im FQDN für die remote erreichbare Adresse vorhanden war (z. B. 'cisco.com' im Vergleich zu 'cisco.com') und die Konfiguration gespeichert werden konnte.
- Da das standardmäßige Nullvertrauensprofil verwendet wurde, d. h. dass jede neu erstellte oder vorhandene private Ressourcenkonfiguration an jeden Benutzer in der Organisation weitergeleitet wird, wurde die Konfiguration mit diesem Leerzeichen synchronisiert. Dieser Leerraum verursachte die "Network Interceptor"-Fehler, die der Client aufwies.
- Um dieses Problem vorerst zu beheben, gehen Sie zu den privaten Ressourcen, und stellen Sie sicher, dass im FQDN der remote erreichbaren Adresse keine Leerzeichen vorhanden sind.

Ursache

Der Netzwerkabfangfehler in Cisco Secure Access Zero Trust Access wird in der Regel durch falsch konfigurierte oder problematische private Ressourcendefinitionen in der ZTNA-Umgebung verursacht. Wenn das remote erreichbare Adressfeld überprüft wurde, gab es einen zusätzlichen Leerraum im FQDN der remote erreichbaren Adresse (z. B. 'cisco.com' im Vergleich zu 'cisco.com').

Verwandte Inhalte

- 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.