

Browserbasierter ZTA-TLS-Handshake für private Ressourcen

Inhalt

Problem

Benutzer können nicht über Cisco Secure Access auf eine browserbasierte private Ressource zugreifen.

Beim Verbindungsversuch treten die folgenden Symptome auf:

- Der TCP-Drei-Wege-Handshake wurde erfolgreich abgeschlossen, aber die TLS-Aushandlung schlägt nach dem Client Hello fehl.
- Die Verbindung mit der öffentlichen, SSE-zugeordneten URL (<https://example-orgid.ztna.sse.cisco.io>) erreicht die Cisco-Authentifizierung, gibt jedoch den HTTP-404-Fehler zurück.
- Nachdem der FQDN zur Konfiguration der privaten Ressource hinzugefügt wurde, wird der Datenverkehr an die Authentifizierungsaufforderung umgeleitet, führt jedoch nach der Authentifizierung zu einer leeren Seite.
- HAR-Dateien zeigen HTTP-200-Antworten, aber der TLS-Handshake wird nicht abgeschlossen.
- Grund für die Sperrung wird angezeigt als: "Private Access: heruntergeladene Statusdaten für Gerät sind zu alt/müssen aktualisiert werden."

Umwelt

- Cisco Secure Access (SSE)
- ID der Organisation für sicheren Zugriff: xxxx
- Browserbasierter Zero Trust Network Access (ZTNA)

- Private Ressource: example.net
- Private Vergleichsressource wird verwendet: abc.net
- Konfiguration des Platzhalterzertifikats

Auflösung

Das Problem wurde behoben, indem die private Ressource so konfiguriert wurde, dass sie dieselbe Zertifikatkonfiguration wie eine funktionierende private Ressource verwendet.

Die in den nächsten Abschnitten beschriebenen Schritte wurden durchgeführt.

Schritt 1: Arbeitskonfiguration analysieren

Vergleichen Sie die ausgefallene private Ressource (example.net) mit einer funktionierenden privaten Ressource (abc.net), um Konfigurationsunterschiede zu ermitteln.

Verwendete Arbeitsressource:

- Option URL in Ihrer Domäne verwenden
- Verweis auf das vorhandene Platzhalterzertifikat/Schlüsselpaar

Phase 2: Paketerfassungsanalyse

Führen Sie eine Paketerfassungsanalyse mit Wireshark durch, um den TLS-Handshake-Fehler zu bestätigen:

- Überprüfen, ob der TCP-Drei-Wege-Handshake erfolgreich abgeschlossen wurde
- Die TLS-Aushandlung kann nach "Client Hello" nicht bestätigt werden.
- Diagnoseartefakte sammeln: HAR-Dateien, DART-Paket und Paketerfassung.

Schritt 3: Zertifikatsüberprüfung

Greifen Sie über die RAVPN-Verbindung auf die Anwendung zu, um die Zertifikatdarstellung zu überprüfen:

- Vergewissern Sie sich, dass die Website example.net ein Platzhalterzertifikat vorlegt.
- Dokumentieren der Zertifikatdetails für die Konfigurationsreferenz

Schritt 4: Private Ressource konfigurieren

Wenden Sie denselben Konfigurationsansatz an, der von der funktionierenden privaten Ressource verwendet wird:

- Konfigurieren Sie die private Ressource für die Option URL in Domäne verwenden.
- Verweisen Sie auf das vorhandene Platzhalterzertifikat/Schlüsselpaar.
- Stellen Sie sicher, dass der FQDN im Feld für private Ressourcen richtig konfiguriert ist.

Schritt 5: Validierung

Testen Sie den browserbasierten Zugriff, um sicherzustellen, dass das Problem durch die Konfiguration gelöst wird:

- Überprüfen des erfolgreichen TLS-Handshake-Abschlusses
- Bestätigen Sie den ordnungsgemäßen Authentifizierungsablauf.
- Validieren Sie den Zugriff auf Anwendungen nach der Authentifizierung.

Ursache

Die Ursache hierfür war eine nicht übereinstimmende Konfiguration in der privaten

Ressourceneinrichtung. Die fehlerhafte private Ressource wurde nicht so konfiguriert, dass sie ordnungsgemäß auf das Platzhalterzertifikat verweist, das von der Zielanwendung präsentiert wurde. Der TLS-Handshake ist fehlgeschlagen, da die private Ressourcenkonfiguration nicht mit der vom Anwendungsserver verwendeten Zertifikatkonfiguration übereinstimmt. Wenn Sie die private Ressource für die Option URL in Domäne verwenden konfigurieren und auf das vorhandene Platzhalterzertifikat/Schlüsselpaar verweisen (entspricht der aktuellen Konfiguration), konnte die TLS-Aushandlung erfolgreich abgeschlossen werden.

Verwandte Inhalte

- [Cisco Referenzhandbuch für sicheren Zugriff](#)
- [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.