Umbrella DNS Security Co-Existenz Probleme mit Broadcom WSS auf macOS

Inhalt

Problem

Das Umbrella-Modul fängt den DNS-Datenverkehr auf macOS nicht ab, wenn es zusammen mit Broadcom WSS (Web Security Service) vorhanden ist. Wenn der WSS-Agent so konfiguriert ist, dass er bestimmte Web-Ports wie 80 und 443 abfängt, erfasst die Umbrella DNS-Sicherheitsfunktion nicht alle DNS-Abfragen. Wenn WSS deaktiviert ist, fängt Umbrella den DNS-Datenverkehr wie erwartet wieder ab. Umbrella verarbeitet nur bestimmte DNS-Abfragen, wenn WSS aktiviert ist, und nicht den gesamten abgefangenen DNS-Verkehr.

Umwelt

- Betriebssystem: MacOS
- Cisco Umbrella DNS Security-Modul
- Broadcom WSS (Web Security Service)-Agent
- WSS-Agent zum Abfangen der Web-Ports 80 und 443 konfiguriert

Auflösung

Dieses Problem wurde analysiert und als architektonische Einschränkung von macOS erkannt, bei der DNS-Sicherheit in der aktuellen macOS-Architektur nicht zusammen mit WSS existieren kann. Diese Einschränkung gilt für die DNS-Sicherheitslösungen Infoblox und Cisco Umbrella.

Technische Analyse

Die Ursache hängt mit den Einschränkungen des macOS DNS-Proxys zusammen:

- Aufgrund von MacOS-Einschränkungen kann jeweils nur ein DNS-Proxy im System aktiv sein.
- Wenn DNS-Resolver an utunX-Schnittstellen oder durch einen Proxy injizierte Resolver gebunden sind, löst macOS DNS im Tunnel auf, nicht über Umbrella
- Wenn ein anderer NEDnsProxyProvider auf dem System von macOS aktiv ist, fängt Umbrella den DNS-Datenverkehr nicht ab

Diagnosebefehle

Verwenden Sie den folgenden Befehl, um zu überprüfen, welcher DNS-Resolver unter macOS Priorität erhält:

```
scutil --dns
```

Mit diesem Befehl wird angezeigt, welcher Resolver wie folgt markiert ist: Umfang, Ergänzung oder Schnittstelle: utunX unterstützt die Identifizierung von DNS-Proxy-Konflikten.

Problemumgehungsoptionen

Für MacOS-Umgebungen wird WSS weiterhin DNS ohne separaten DNS-Agent abfangen. Um die DNS-Sicherheit voranzutreiben, könnte eine der Optionen die Implementierung einer passiven Bypass-Architektur sein. Bei diesem Ansatz würde der Provider den Datenfluss vollständig umgehen, sodass der Datenverkehr so verarbeitet werden kann, als wäre er nicht aktiv.

Ursache

Das Problem wird durch macOS-Architektureinschränkungen verursacht, bei denen jeweils nur ein NEDnsProxyProvider auf dem System aktiv sein kann. Wenn sowohl Umbrella DNS Security als auch Broadcom WSS installiert sind, konkurrieren sie um die DNS-Proxy-Steuerung, was dazu führt, dass WSS Priorität erhält und Umbrella den DNS-Datenverkehr nicht abfängt. Dies ist eine grundlegende Einschränkung des macOS-Netzwerk-Stacks und betrifft alle DNS-Sicherheitslösungen, nicht nur Cisco Umbrella.

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.