Fragmentierte ICMP-Paketverarbeitung für sicheren Zugriff von Cisco

Inhalt

Problem

ICMP-Echo-Anfragen, die größer als die MTU sind, erhalten keine Antworten, wenn das DF-Bit (Nicht fragmentieren) deaktiviert ist. Dieses Verhalten tritt in zwei spezifischen Szenarien auf:

- Von RAVPN-Endpunkten über die VPN-Schnittstelle beim Senden von ICMP-Paketen, die die MTU-Größe der VPN-Schnittstelle mit gelöschtem DF-Bit überschreiten
- Von Endpunkten vor Ort über einen IPsec-Tunnel zwischen einem Router am Standort und Cisco Secure Access (CSA) beim Senden von ICMP-Paketen, die die MTU-Größe der IPsec-Tunnelschnittstelle bei gelöschtem DF-Bit überschreiten

In beiden Fällen werden keine ICMP-Antworten empfangen, was zu Fragen darüber führt, ob CSA fragmentierte Pakete mit deaktiviertem DF-Bit verwirft.

Umwelt

- Cisco Secure Access (CSA)
- RAVPN-Endgeräte (Remote Access VPN)
- IPsec-Tunnel zwischen Standort-Routern und CSA
- ICMP-Datenverkehr überschreitet MTU-Schnittstellengrößen
- Fragmentierte Paketszenarien mit gelöschtem DF-Bit

Auflösung

Cisco Secure Access verwirft fragmentierte Pakete in Underlay- und Overlay-Szenarien. Dieses Verhalten wird in der Cisco Secure Access-Hilfe dokumentiert, die explizit Folgendes angibt:

"Fragmentierte Pakete im Underlay oder Overlay werden verworfen."

Erwartetes Verhalten

Cisco Secure Access wurde entwickelt, um fragmentierte Pakete zu verwerfen, unabhängig davon, ob sie sich im Underlay- oder Overlay-Netzwerk befinden. Dies gilt für:

- Von RAVPN-Endpunkten gesendete ICMP-Pakete, die die MTU der VPN-Schnittstelle überschreiten, wobei das DF-Bit gelöscht wird
- ICMP-Pakete, die von Endpunkten vor Ort über IPsec-Tunnel gesendet werden und die MTU der Tunnelschnittstelle mit DF-Bit-Bereinigung überschreiten

Dieses Verhalten ist in allen Szenarien mit fragmentierten Paketen innerhalb der Cisco Secure Access-Infrastruktur gleich.

Hierfür wurde die Funktionsanfrage CSE-I-5739 erstellt.

Ursache

Cisco Secure Access wurde so konzipiert, dass fragmentierte Pakete als Entscheidung für ein Sicherheits- und Leistungs-Design verworfen werden. Dieses Verhalten wird implementiert, um potenzielle Sicherheitsschwachstellen und Verarbeitungsaufwand zu vermeiden, der mit der Paketreassemblierung sowohl in Underlay- als auch in Overlay-Netzwerkszenarien verbunden ist.

Verwandte Inhalte

- Cisco Secure Access-Hilfedokumentation - Fragmentierte Paketverarbeitung
- 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.