

DLP-Richtlinieneinschränkungen mit WhatsApp für sicheren Zugriff

Inhalt

Problem

DLP-Richtlinien in Cisco Secure Access erkennen oder blockieren vertrauliche Dateien nicht, wenn sie über WhatsApp (Browser oder Desktop-Anwendung) freigegeben werden, obwohl die HTTPS-Entschlüsselung aktiviert ist. Das DLP-Modul löst keine Datei-Uploads über diese Plattformen aus oder erkennt diese nicht, während dieselben DLP-Richtlinien identische Dateien erfolgreich blockieren, wenn sie über andere Online-Upload-Tools hochgeladen werden. Beim Testen der grundlegenden Upload-Blockierung für WhatsApp funktioniert die Funktion sowohl auf Browser- als auch auf Desktopversionen ordnungsgemäß. Das Problem ist jedoch speziell auf die Durchsetzung von DLP-Richtlinien beschränkt.

Umwelt

- Sicherer Zugriff von Cisco
- SvD-Policys konfiguriert
- HTTPS-Entschlüsselung aktiviert
- WhatsApp Web- und WhatsApp Desktop-Anwendungen

Auflösung

Das beobachtete Verhalten ist eine erwartete Einschränkung von WhatsApp und ähnlichen Plattformen aufgrund ihrer End-to-End-Verschlüsselung (E2EE) Implementierung und nicht standardmäßigen Datenverkehrsbehandlung. Die in den nächsten Abschnitten beschriebenen Schritte zur Fehlerbehebung und die Problemumgehung können implementiert werden.

Schritte zur Fehlerbehebung

Überprüfen Sie vor der Implementierung der Problemumgehung die folgenden Konfigurationselemente:

- Stellen Sie sicher, dass die richtige SWG-Identitäts-/Ursprungs-ID konfiguriert ist.
- Vergewissern Sie sich, dass die HTTPS-Inspektion/-Entschlüsselung für die Zielplattformen aktiviert und nicht selektiv umgangen wird.
- Überprüfen Sie, ob die Einstellungen für Isolierung/RBI und Allow-Override ordnungsgemäß konfiguriert sind.
- Bestätigen Sie die AD-Gruppenmitgliedschaft, wenn SvD-Policys gruppenbasiert sind.
- Prüfen Sie die Umgehungslisten für die Verkehrssteuerung auf mögliche Ausnahmen.
- Überprüfen, ob das QUIC-Protokoll in Browsern deaktiviert ist
- Überprüfen Sie, ob der IPv6-Datenverkehr Auswirkungen hat, die eine Überprüfung umgehen könnten.

Empfohlene Lösung

Um die DLP-Durchsetzung für WhatsApp-Webdatenverkehr zu aktivieren, implementieren Sie Remote Browser Isolation (RBI) für Datenverkehr, der an WhatsApp Web gerichtet ist. Diese Problemumgehung ermöglicht die Durchsetzung von DLP-Richtlinien, indem die Browser-Sitzung isoliert wird und die Inhaltsüberprüfung in der isolierten Umgebung aktiviert wird.

Konfigurieren Sie die RBI-Durchsetzung speziell für WhatsApp-Webdomänen, um sicherzustellen, dass Datei-Uploads und die Inhaltsfreigabe über die Webschnittstelle einer DLP-Richtlinienauswertung unterliegen.

Zusätzliche Informationen

Es wurde ein Antrag auf Produktverbesserung für diese Beschränkung dokumentiert - CSE-I-1249.

Ursache

WhatsApp (einschließlich WhatsApp Web) und ähnliche Collaboration-Plattformen implementieren End-to-End-Verschlüsselung (E2EE), die eine vollständige Inhaltsüberprüfung und das Scannen von Nachrichtentexten und Datei-Uploads verhindert. Darüber hinaus nutzt der WhatsApp-Datenverkehr standardmäßige HTTP-/HTTPS-Ports nicht in der gleichen Weise wie herkömmliche Web-Uploads. Das bedeutet, dass das Secure Web Gateway (SWG) den Datenverkehr über den normalen HTTPS-Prüfpfad nicht abfangen und überprüfen kann. Diese Verschlüsselungs- und Datenverkehrsverarbeitungsmethode ist vom Design und stellt eine erwartete Einschränkung der aktuellen DLP-Überprüfungsfunktionen für diese spezifischen Plattformen dar.

Verwandte Inhalte

- [Anfrage für Produkterweiterung CSE-I-1249](#)
- [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.