

DLP-beleidsbeperkingen met WhatsApp in beveiligde toegang

Inhoud

uitgifte

DLP-beleid in Cisco Secure Access detecteert of blokkeert geen gevoelige bestanden wanneer deze worden gedeeld via WhatsApp (browser- of desктоptoepassing), ondanks dat HTTPS-decodering is ingeschakeld. De DLP-engine activeert of detecteert geen bestandsuploads via deze platforms, terwijl hetzelfde DLP-beleid met succes identieke bestanden blokkeert wanneer deze worden geüpload via andere online uploadtools. Bij het testen van elementaire uploadblokkering voor WhatsApp werkt de functionaliteit correct op zowel browser- als desktopversies, maar het probleem is specifiek geïsoleerd voor DLP-beleidshandhaving.

milieu

- Cisco Secure Access
- DLP-beleid geconfigureerd
- HTTPS-decryptie ingeschakeld
- WhatsApp Web en WhatsApp Desktop applicaties

resolutie

Het waargenomen gedrag is een verwachte beperking van WhatsApp en vergelijkbare platforms vanwege hun end-to-end encryptie (E2EE) -implementatie en niet-standaard verkeersverwerking. De stappen voor het oplossen van problemen die in de volgende secties en in de workaround worden beschreven, kunnen worden geïmplementeerd.

Verificatiestappen voor problemen oplossen

Voordat u de tijdelijke oplossing implementeert, controleert u de volgende configuratie-items:

- Zorg ervoor dat de juiste SWG-identiteit/oorsprong-ID is geconfigureerd.
- Bevestig dat HTTPS-inspectie/decryptie is ingeschakeld en niet selectief is omzeild voor de doelplatforms.
- Controleer of de instellingen Isolation/RBI en Allow-Override correct zijn geconfigureerd.
- Bevestig het lidmaatschap van een AD-groep als het DLP-beleid op groepen is gebaseerd.
- Controleer de bypass-lijsten van Traffic Steering voor eventuele uitsluitingen.
- Controleer of het QUIC-protocol is uitgeschakeld in browsers.
- Controleer op IPv6-verkeerseffecten die inspectie kunnen omzeilen.

Aanbevolen workaround

Om DLP-handhaving voor WhatsApp-webverkeer mogelijk te maken, implementeert u Remote Browser Isolation (RBI) voor verkeer dat bestemd is voor WhatsApp Web. Deze workaround maakt het mogelijk om DLP-beleid af te dwingen door de browsersessie te isoleren en inhoudsinspectie in de geïsoleerde omgeving mogelijk te maken.

Configureer RBI-handhaving specifiek voor WhatsApp-webdomeinen om ervoor te zorgen dat het uploaden van bestanden en het delen van inhoud via de webinterface onderworpen zijn aan de evaluatie van het DLP-beleid.

Aanvullende informatie

Voor deze beperking is een verzoek voor productverbetering gedocumenteerd - CSE-I-1249.

Oorzaak

WhatsApp (inclusief WhatsApp Web) en vergelijkbare samenwerkingsplatforms implementeren end-to-end encryptie (E2EE) die volledige inhoudsinspectie en het scannen van berichttekst en bestandsuploads voorkomt. Bovendien maakt WhatsApp-verkeer geen gebruik van standaard HTTP / HTTPS-poorten op dezelfde manier als typische webuploads, wat betekent dat de Secure Web Gateway (SWG) het verkeer niet kan onderscheppen en inspecteren via het normale HTTPS-inspectiepad. Deze versleutelings- en verkeersverwerkingsmethode is ontworpen en vertegenwoordigt een verwachte beperking van de huidige DLP-inspectiemogelijkheden voor deze specifieke platforms.

Gerelateerde inhoud

- [Aanvraag voor productverbetering CSE-I-1249](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.