

Limitazioni dei criteri di prevenzione della perdita dei dati con WhatsApp in Secure Access

Sommario

Problema

I criteri di prevenzione della perdita dei dati in Cisco Secure Access non rilevano o bloccano i file riservati quando vengono condivisi tramite WhatsApp (browser o applicazione desktop), nonostante sia abilitata la decrittografia HTTPS. Il motore di prevenzione della perdita dei dati non è in grado di attivare o rilevare caricamenti di file attraverso queste piattaforme, mentre gli stessi criteri di prevenzione della perdita dei dati bloccano file identici quando caricati tramite altri strumenti di caricamento online. Durante il test del blocco di caricamento di base per WhatsApp, la funzionalità funziona correttamente sia sul browser che sul desktop, ma il problema è specificamente isolato per l'applicazione dei criteri di prevenzione della perdita dei dati.

Ambiente

- Cisco Secure Access
- Criteri DLP configurati
- Decrittografia HTTPS abilitata
- Applicazioni WhatsApp Web e WhatsApp Desktop

Risoluzione

Il comportamento osservato è una limitazione prevista di WhatsApp e piattaforme simili a causa dell'implementazione della crittografia end-to-end (E2EE) e della gestione del traffico non standard. È possibile implementare le procedure di risoluzione dei problemi descritte nelle sezioni seguenti e la soluzione alternativa proposta.

Procedura di verifica per la risoluzione dei problemi

Prima di implementare la soluzione, verificare i seguenti elementi di configurazione:

- Assicurarsi che l'ID di origine/identità SWG sia configurato correttamente.
- Confermare che l'ispezione/decriptografia HTTPS sia abilitata e non ignorata in modo selettivo per le piattaforme di destinazione.
- Verificare che le impostazioni Isolation/RBI e Allow-Override siano configurate correttamente.
- Confermare l'appartenenza al gruppo AD se i criteri di prevenzione della perdita dei dati sono basati su gruppo.
- Controllare gli elenchi di bypass del Traffic Steering per eventuali esclusioni.
- Verificare che il protocollo QUIC sia disattivato nei browser.
- Verificare gli effetti del traffico IPv6 che potrebbero ignorare l'ispezione.

Soluzione consigliata

Per abilitare l'imposizione dei criteri di prevenzione della perdita dei dati per il traffico Web WhatsApp, implementare l'isolamento del browser remoto (RBI, Remote Browser Isolation) per il traffico destinato al Web WhatsApp. Questa soluzione consente di applicare le policy di prevenzione della perdita dei dati isolando la sessione del browser e abilitando l'ispezione dei contenuti all'interno dell'ambiente isolato.

Configurare l'imposizione RBI specificamente per i domini Web WhatsApp per garantire che i caricamenti di file e la condivisione di contenuto tramite l'interfaccia Web siano soggetti alla valutazione dei criteri di prevenzione della perdita dei dati.

Ulteriori informazioni

È stata documentata una richiesta di miglioramento del prodotto per questa limitazione - CSE-I-1249.

Causa

WhatsApp (incluso WhatsApp Web) e piattaforme di collaborazione simili implementano la crittografia end-to-end (E2EE) che impedisce l'ispezione completa dei contenuti e la scansione del testo dei messaggi e il caricamento dei file. Inoltre, il traffico WhatsApp non utilizza le porte HTTP/HTTPS standard allo stesso modo dei tipici caricamenti Web, il che significa che il Secure Web Gateway (SWG) non può intercettare e ispezionare il traffico attraverso il normale percorso di ispezione HTTPS. Questo metodo di cifratura e gestione del traffico è progettato e rappresenta un limite previsto delle attuali funzionalità di ispezione dei DLP per queste piattaforme specifiche.

Contenuto correlato

- [Richiesta di miglioramento del prodotto CSE-I-1249](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).