Configurazione del comportamento di chiusura non riuscita del DLP che blocca le azioni utente durante la perdita di connettività del cloud

Sommario

Problema

Un utente con il modulo EDLP (Endpoint DLP) installato stava riscontrando il blocco della stampa e della copia nelle condivisioni di file di rete, nonostante non fosse incluso in alcuna regola EDLP configurata. Tutte le regole EDLP esistenti sono state configurate in modalità MONITOR con solo 3 utenti specifici inclusi in tali regole. L'utente interessato ha rilevato azioni di blocco impreviste per operazioni di stampa e di copia di condivisione file, anche se non erano destinate a essere soggette all'applicazione EDLP.

Durante la risoluzione dei problemi, è stato determinato che il blocco si è verificato quando la connettività cloud EDLP non era disponibile, causando l'applicazione da parte del sistema del comportamento fail-closed come meccanismo di fallback. L'utente ha riscontrato il rifiuto della stampa e dell'accesso alla condivisione di rete durante i periodi in cui il client EDLP non ha stabilito la connettività al servizio cloud per i verdetti dei criteri.

Ambiente

- Modulo Cisco Endpoint DLP versione 1.5.0.292
- Gestione del portale Cisco Secure Access/Secure/Data Loss Prevention
- Più regole EDLP configurate in modalità MONITOR
- Canale di condivisione di rete configurato con comportamento di chiusura a causa di errori
- Modifiche alla risoluzione DNS che influiscono sulla connettività di rete dei client

Risoluzione

La risoluzione ha comportato la comprensione e la spiegazione del comportamento di chiusura di errore dell'EDLP e della relativa applicazione durante la perdita di connettività cloud:

Analisi della causa principale

L'analisi del bundle DART e dei log EDLP ha rivelato che EDLP ha applicato un fallback di negazione perché il canale della condivisione di rete era configurato come chiuso in caso di errore. Al momento del blocco degli incidenti, la connettività cloud EDLP non era disponibile a causa di modifiche alla risoluzione DNS nella rete client, impedendo al sistema di ottenere i verdetti dei criteri dal servizio cloud.

Spiegazione del comportamento di chiusura degli errori

Il criterio di chiusura non riuscita è stato applicato al sistema dell'utente perché è stato installato il modulo EDLP, indipendentemente dal fatto che l'identità dell'utente fosse inclusa in una regola EDLP specifica. Lo stato fail-open/fail-closed è un'impostazione globale fornita nella configurazione dei criteri di prevenzione della perdita dei dati e la configurazione del canale viene applicata in base a tale impostazione globale.

Ripristino connettività

Il problema è stato risolto automaticamente dopo il ripristino della stabilità DNS nella rete del client, consentendo al client EDLP di ristabilire la connettività al servizio cloud. Non è stato necessario alcun intervento manuale una volta risolto il problema di connettività di rete sottostante.

Condizioni che causano la chiusura forzata

Queste condizioni possono attivare il comportamento di chiusura di errore di EDLP:

- Problemi di risoluzione DNS
- Interruzioni della rete
- Passaggio da una rete all'altra
- Qualsiasi condizione che impedisce la connessione end-to-end tra il client e il servizio cloud

Causa

Il comportamento di blocco è stato causato dalla configurazione con chiusura a errori di EDLP per il canale della condivisione di rete. Quando il client EDLP ha perso la connettività al servizio cloud a causa di modifiche della risoluzione DNS, non può ottenere verdetti sui criteri e pertanto applica il comportamento di chiusura degli errori configurato come meccanismo di fallback della sicurezza. Ciò si è verificato indipendentemente dal fatto che l'utente sia stato esplicitamente incluso in qualsiasi regola di EDLP, in quanto l'impostazione di chiusura con errori si applica globalmente a tutti i sistemi con il modulo EDLP installato quando la connettività cloud non è disponibile.

Contenuto correlato

- 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).