Configurazione della scansione antivirus ESA dopo la rimozione dell'allegato

Sommario

Introduzione

In questo documento viene descritto se la scansione dei software antivirus rimane necessaria dopo la rimozione degli allegati da Cisco Email Security Appliance (ESA).

Premesse

La scansione antivirus deve rimanere abilitata su Cisco Email Security Appliance (ESA) anche quando le regole per la rimozione degli allegati sono abilitate, in quanto la rimozione degli allegati non rimuove in modo affidabile tutto il contenuto dannoso da ogni struttura dei messaggi.

Dichiarazione di problema

Gli amministratori possono supporre che la rimozione degli allegati elimina il rischio di malware e rende superflua la scansione antivirus. In questo documento viene illustrato il motivo per cui è necessario continuare a utilizzare la scansione antivirus dopo la rimozione degli allegati.

Ambiente

Le presenti linee guida si applicano ai messaggi e-mail in entrata e in uscita elaborati da Cisco Email Security Appliance (ESA).

Suggerimento

La scansione antivirus è richiesta per i messaggi anche quando le regole per la rimozione degli allegati sono abilitate su Cisco Email Security Appliance (ESA).

Mantenere la scansione antivirus abilitata per tutti i flussi di posta applicabili dopo la configurazione dei criteri di rimozione degli allegati.

- Analizza i messaggi e-mail in arrivo perché è possibile che nelle parti del messaggio rimangano contenuti dannosi che non vengono rimossi dalle regole per l'eliminazione degli allegati.
- Analizza i messaggi e-mail in uscita perché possono ancora contenere malware dopo l'elaborazione della rimozione degli allegati.
- Regole per la rimozione degli allegati per ridurre i rischi e non per sostituire la scansione antivirus.

Nota: Risultato previsto: la rimozione degli allegati può ridurre l'esposizione ad alcune minacce basate su file, ma è comunque necessaria la scansione antivirus per rilevare il contenuto dannoso che rimane nel messaggio. Ambito: le presenti linee guida indicano se è ancora necessaria la scansione antivirus dopo la rimozione degli allegati; non descrive tutte le funzionalità di rilevamento di malware su ESA.

Perché la rimozione degli allegati non è sufficiente

La perdita di allegati riduce i rischi ma non li elimina.

- L'allegato non è una definizione tecnica rigorosa.
- L'ESA valuta le parti MIME definite dall'RFC, non un oggetto di collegamento universale.
- I messaggi possono essere costruiti in modo da ignorare la logica dell'allegato-dropping perché il termine "allegato" non è una definizione tecnica precisa.
- Poiché il contenuto e-mail può essere strutturato in diversi formati MIME, le regole per la rimozione degli allegati non consentono di rimuovere in modo affidabile tutto il contenuto dannoso.
- La posta in uscita può ancora trasportare malware.

Informazioni correlate

Per ulteriori informazioni, vedere:

- Descrizioni delle azioni del filtro messaggi ESA
- Utilizzo dei filtri messaggi

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).