Correggi errori di visualizzazione pagina EUN in SWA per richieste HTTPS esplicite

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il problema di visualizzazione non corretta delle pagine EUN nell'interfaccia SWA di Cisco per le richieste HTTPS esplicite.

Prerequisiti

Requisiti

Le informazioni fornite in questo documento presuppongono che:

- L'appliance Web sicura (SWA) viene distribuita in modalità esplicita.
- SWA è in esecuzione sulle versioni 7.7.0 e precedenti.
- Le richieste HTTPS sono bloccate, avvisate o richiedono conferma da parte dell'utente.
- La decrittografia HTTPS è abilitata.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Le pagine Avviso, Conferma o Notifica utente finale non vengono visualizzate correttamente per le richieste HTTPS esplicite. Il browser visualizza una pagina di notifica incompleta oppure non

visualizza affatto la pagina e visualizza una pagina di errore.

Quando si utilizzano richieste HTTPS esplicite, in queste pagine sono presenti diversi problemi. Quando si configura il browser per l'utilizzo di un proxy, il traffico HTTPS viene indirizzato al server SWA tramite HTTP. La richiesta è formattata come HTTPS su HTTP.

Esistono due problemi noti con i browser che non gestiscono correttamente le risposte HTTP restituite dal file SWA per le richieste HTTPS esplicite:

1. Quando una richiesta HTTPS esplicita viene bloccata, avvisata o richiede la conferma dell'utente, l'SWA restituisce un codice di stato HTTP/403.
2. All'interno di questa risposta, l'SWA include il contenuto della notifica che normalmente deve essere visualizzato sullo schermo in modo che sia visualizzabile. Tuttavia, in alcuni casi, il browser non è in grado di comprendere la risposta all'interno del contenuto restituito.

Questo è il comportamento del browser osservato:

- Quando si utilizza Internet Explorer versione 6 (IE6) e alcune versioni di IE7, queste richieste non consentono di eseguire il rendering dell'intero contenuto della risposta HTML. Il browser rispetta solo i primi byte (il contenuto all'interno del primo pacchetto) e ignora il resto. In questi casi, viene visualizzata una pagina incompleta che contiene solo pochi caratteri.

Nota: In questo caso, Cisco consiglia di ridurre la pagina di notifica predefinita dalla risposta SWA. Per ulteriori informazioni su come modificare la pagina EUN, consultare la sezione Modifica dei file HTML della pagina di notifica direttamente nella Guida dell'utente SWA.

- Quando si usano IE8 e le versioni più recenti di Mozilla Firefox Release 3, il browser ignora completamente la risposta che l'SWA restituisce e la maschera con la propria pagina di errore. Questo comportamento del browser vanifica lo scopo della notifica 403 e causa interruzioni con la funzione.

Soluzione

In questa sezione viene descritto il processo che si verifica quando la decrittografia HTTPS è abilitata nell'SWA. Questo problema è stato risolto nella versione SWA 7.7.0-500 e successive (ID bug Cisco CSCzv25138) Per risolvere il problema descritto in precedenza, utilizzare le informazioni fornite in modo da verificare che il sistema sia configurato di conseguenza.

Di seguito è riportato un esempio del flusso di traffico quando viene inviata una richiesta HTTPS esplicita:

- Quando la decrittografia HTTPS è abilitata, l'SWA convalida innanzitutto la richiesta in base ai criteri di decrittografia.

- Se la richiesta è contrassegnata per PASSTHROUGH, il traffico viene autorizzato (senza

avviso o EUN).

- Se la richiesta è contrassegnata come DECRITTOGRAFATA, viene convalidata in base ai criteri di accesso. In questo caso, se i criteri di accesso sono configurati in modo da WARN o BLOCK, la pagina EUN viene visualizzata correttamente. Per Conferma, l'utente deve passare alla pagina HTTP e Conferma, che richiede la navigazione attraverso il proxy e quindi al sito HTTPS.

- L'SWA ricorda l'indirizzo IP del client e non richiede un'altra conferma fino alla scadenza del timer.

Informazioni correlate

- Guida per l'utente di AsyncOS 14.5 per Cisco Secure Web Appliance - GD (General Deployment) - Cisco

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).