

Fouten in de weergave van EUN-pagina's op SWA voor expliciete HTTPS-verzoeken oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het probleem van EUN-pagina's die onjuist worden weergegeven op de Cisco SWA voor expliciete HTTPS-verzoeken.

Voorwaarden

Vereisten

De informatie in dit document gaat ervan uit dat:

- De Secure Web Appliance (SWA) wordt geïmplementeerd in de explicieteodus.
- De SWA wordt uitgevoerd op versie 7.7.0 en eerder.
- De HTTPS-verzoeken worden geblokkeerd, gewaarschuwd of vereisen gebruikersbevestiging.
- HTTPS-decodering is ingeschakeld.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

De pagina's Waarschuwing, Bevestiging of Melding voor eindgebruikers (EUN) worden niet correct

weergegeven voor expliciete HTTPS-verzoeken. De browser geeft een onvolledige meldingspagina weer, of de pagina wordt helemaal niet weergegeven en in plaats daarvan wordt een foutpagina weergegeven.

Er zijn verschillende problemen die deze pagina's omringen wanneer u expliciete HTTPS-verzoeken gebruikt. Wanneer u uw browser configureert om een proxy te gebruiken, wordt HTTPS-verkeer naar de SWA via HTTP geleid. Dit verzoek is geformatteerd als een HTTPS over HTTP.

Er zijn twee bekende problemen met browsers die niet correct omgaan met de HTTP-antwoorden die de SWA retourneert voor expliciete HTTPS-verzoeken:

1. Wanneer een expliciet HTTPS-verzoek wordt geblokkeerd, gewaarschuwd of een gebruikersbevestiging vereist, retourneert de SWA een HTTP/403-statuscode.
2. In dit antwoord bevat de SWA de meldingsinhoud die normaal gesproken op het scherm moet worden weergegeven, zodat deze zichtbaar is. In sommige gevallen kan de browser het antwoord echter niet begrijpen binnen de getourneerde inhoud.

Dit is het browsergedrag dat wordt waargenomen:

- Wanneer Internet Explorer versie 6 (IE6) en sommige versies van IE7 worden gebruikt, slagen deze verzoeken er niet in de volledige inhoud van het HTML-antwoord weer te geven. De browser honoreert alleen de eerste paar bytes (de inhoud in het eerste pakket) en negeert de rest. In dergelijke gevallen ziet u een onvolledige pagina die slechts een paar tekens weergeeft.



Opmerking: Als dit het geval is, raadt Cisco u aan de standaardmeldingspagina te verkleinen van het SWA-antwoord. Voor meer informatie over het bewerken van uw EUN-pagina, raadpleegt u het gedeelte HTML-bestanden direct bewerken van de SWA-gebruikershandleiding.

- Wanneer IE8 en nieuwere versies van Mozilla Firefox Release 3 worden gebruikt, negeert de browser volledig het antwoord dat de SWA retourneert en maskeert deze met zijn eigen foutpagina. Dit browsergedrag verslaat het doel van de 403-melding en veroorzaakt verstoring van de functie.

Oplossing

In dit gedeelte wordt het proces beschreven dat optreedt wanneer HTTPS-decoding is ingeschakeld op de SWA. Dit probleem is verholpen in SWA versie 7.7.0-500 en hoger (Cisco bug ID [CSCzv25138](#)). Gebruik de verstrekte informatie als oplossing voor het eerder beschreven probleem om ervoor te zorgen dat uw systeem dienovereenkomstig is geconfigureerd.

Hier is een voorbeeld van de verkeersstroom wanneer een expliciet HTTPS-verzoek wordt verzonden:

- Wanneer HTTPS-decodering is ingeschakeld, valideert de SWA eerst het verzoek met het decoderingsbeleid.
- Als het verzoek is gemarkeerd voor PASSTHROUGH, dan is het verkeer toegestaan door (geen waarschuwing of EUN).
- Als het verzoek is gemarkeerd als GEDECODEERD, wordt het verzoek gevalideerd aan de hand van het toegangsbeleid. Als het toegangsbeleid is geconfigureerd om te WAARSCHUWEN of BLOKKEREN, wordt de pagina EUN correct weergegeven. Helaas moet de gebruiker voor de bevestiging naar de HTTP-pagina en Bevestigen navigeren, waarvoor navigatie door de proxy en vervolgens naar de HTTPS-site vereist is.
- De SWA onthoudt het IP-adres van de client en vereist geen nieuwe bevestiging totdat de timer is verlopen.

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Appliance - GD \(Algemene implementatie\) - Cisco](#)

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.