WSA-Warnung, -Bestätigung und -EUN-Seiten werden für explizite HTTPS-Anforderungen nicht korrekt angezeigt

Inhalt

Einführung

Dieses Dokument beschreibt ein Problem, das auf der Cisco Web Security Appliance (WSA) auftritt, wenn die Seiten Warning (Warnung), Acknowledgement (Bestätigung) oder End User Notification (EUN) für explizite HTTPS-Anforderungen nicht korrekt angezeigt werden. Eine Lösung für dieses Problem wird ebenfalls bereitgestellt.

Voraussetzungen

Anforderungen

Die Informationen in diesem Dokument gehen davon aus, dass:

- Die WSA-Proxyadressen werden im expliziten Modus bereitgestellt.
- Die HTTPS-Anforderungen werden entweder blockiert, gewarnt oder erfordern eine Bestätigung durch den Benutzer.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco WSA.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Die Seiten Warnung, Bestätigung oder EUN werden für explizite HTTPS-Anforderungen nicht korrekt angezeigt. Der Browser zeigt eine unvollständige Benachrichtigungsseite an, oder er zeigt die Seite überhaupt nicht an und zeigt stattdessen eine Fehlerseite an.

Es gibt mehrere Probleme, die diese Seiten umschließen, wenn Sie explizite HTTPS-Anforderungen verwenden. Wenn Sie Ihren Browser so konfigurieren, dass er einen Proxy verwendet, wird der HTTPS-Datenverkehr über HTTP an die WSA weitergeleitet. Diese Anforderung wird als HTTPS über HTTP formatiert.

Es gibt zwei bekannte Probleme mit Browsern, die die HTTP-Antworten, die die WSA für explizite HTTPS-Anforderungen zurückgibt, nicht korrekt behandeln. Wenn eine explizite HTTPS-Anforderung entweder blockiert, gewarnt oder eine Bestätigung durch den Benutzer erfordert, gibt die WSA einen 403-Statuscode zurück. In dieser Antwort enthält die WSA den Benachrichtigungsinhalt, der normalerweise auf dem Bildschirm angezeigt werden sollte, damit er angezeigt werden kann. In einigen Fällen kann der Browser die Antwort jedoch nicht in den zurückgegebenen Inhalten verstehen.
Dies ist das beobachtete Browserverhalten:

- Wenn Internet Explorer 6 (IE6) und einige Versionen von IE7 verwendet werden, können diese Anforderungen nicht den gesamten Inhalt der HTML-Antwort wiedergeben. Der Browser berücksichtigt nur die ersten paar Byte (den Inhalt innerhalb des ersten Pakets) und ignoriert den Rest. In solchen Fällen wird eine unvollständige Seite angezeigt, die nur wenige Zeichen enthält.
  Hinweis: In diesem Fall empfiehlt Cisco, die Standard-Benachrichtigungsseite von der WSA-Antwort zu verkleinern. Weitere Informationen zum Bearbeiten der EUN-Seite finden Sie im Abschnitt **Bearbeiten von IronPort-Benachrichtigungsseiten** im **WSA-Benutzerhandbuch**.
- Wenn IE8 und neuere Versionen von Mozilla Firefox Release 3 verwendet werden, ignoriert der Browser die Antwort, die die WSA zurückgibt, völlig und maskiert sie mit einer eigenen Fehlerseite. Dieses Browserverhalten besiegt den Zweck der 403-Benachrichtigung und verursacht eine Unterbrechung der Funktion.

Lösung

In diesem Abschnitt wird der Prozess beschrieben, der auftritt, wenn die HTTPS-Entschlüsselung auf der WSA aktiviert ist. Verwenden Sie als Problemumgehung die bereitgestellten Informationen, um sicherzustellen, dass Ihr System entsprechend konfiguriert ist.

Das folgende Beispiel zeigt den Datenverkehrsfluss, wenn eine explizite HTTPS-Anforderung gesendet wird:

- Wenn die HTTPS-Entschlüsselung aktiviert ist, validiert die WSA die Anforderung zuerst anhand der Entschlüsselungsrichtlinien.

- Wenn die Anforderung für **PASSTHROUGH** markiert ist, wird der Datenverkehr durchgelassen (keine Warnung oder EUN).

- Wenn die Anforderung als **DECRYPTED** markiert ist, wird die Anforderung anhand der

Zugriffsrichtlinien validiert. Wenn in diesem Fall die Zugriffsrichtlinie so konfiguriert ist, dass **WARN** oder **BLOCK** erfolgt, wird die Seite EUN richtig angezeigt. Leider muss der Benutzer zur Bestätigung zur HTTP-Seite und zur Bestätigung navigieren. Dies erfordert die Navigation durch den Proxy und dann zur HTTPS-Website.

- Die WSA speichert die Client-IP-Adresse und benötigt bis zum Ablauf des Timers keine weitere Bestätigung.