Beheben von Fehlern bei der EUN-Seitenanzeige in SWA für explizite HTTPS-Anforderungen

Inhalt

Einleitung

In diesem Dokument wird das Problem beschrieben, dass EUN-Seiten im Cisco SWA für explizite HTTPS-Anforderungen falsch angezeigt werden.

Voraussetzungen

Anforderungen

Bei den Informationen in diesem Dokument wird Folgendes vorausgesetzt:

- Die Secure Web Appliance (SWA) wird im expliziten Modus bereitgestellt.
- Die SWA wird auf Version 7.7.0 und früheren Versionen ausgeführt.
- Die HTTPS-Anfragen werden entweder blockiert, es wird eine Warnung ausgegeben oder die Bestätigung des Benutzers wird benötigt.
- HTTPS-Entschlüsselung ist aktiviert.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Die Seiten Warning (Warnung), Acknowledgement (Bestätigung) (Endbenutzerbenachrichtigung) (EUN) werden für explizite HTTPS-Anforderungen nicht richtig angezeigt. Der Browser zeigt eine unvollständige Benachrichtigungsseite oder gar keine Seite an und zeigt stattdessen eine Fehlerseite an.

Bei expliziten HTTPS-Anforderungen sind diese Seiten von mehreren Problemen umgeben. Wenn Sie Ihren Browser für die Verwendung eines Proxys konfigurieren, wird der HTTPS-Datenverkehr über HTTP an den SWA weitergeleitet. Diese Anforderung wird als HTTPS über HTTP formatiert.

Es gibt zwei bekannte Probleme mit Browsern, die die HTTP-Antworten, die der SWA für explizite HTTPS-Anforderungen zurückgibt, nicht korrekt verarbeiten:

1. Wenn eine explizite HTTPS-Anfrage blockiert wird, eine Warnung ausgibt oder eine Bestätigung durch den Benutzer erfordert, gibt der SWA einen HTTP/403-Statuscode zurück.
2. Innerhalb dieser Antwort enthält der SWA die Benachrichtigungsinhalte, die normalerweise auf dem Bildschirm angezeigt werden müssen. In einigen Fällen kann der Browser jedoch die Antwort innerhalb des zurückgegebenen Inhalts nicht verstehen.

Dies ist das Verhalten des Browsers, das beobachtet wurde:

- Wenn Internet Explorer 6 (IE6) und einige Versionen von IE7 verwendet werden, können diese Anforderungen den vollständigen Inhalt der HTML-Antwort nicht wiedergeben. Der Browser erkennt nur die ersten Bytes (den Inhalt des ersten Pakets) und ignoriert den Rest. In diesem Fall wird eine unvollständige Seite angezeigt, auf der nur wenige Zeichen angezeigt werden.

  Anmerkung: In diesem Fall empfiehlt Cisco, die Standardbenachrichtigungsseite für die SWA-Antwort zu verkleinern. Weitere Informationen zum Bearbeiten der EUN-Seite finden Sie im Abschnitt Direkte Bearbeitung von HTML-Dateien der Benachrichtigungsseite im SWA-Benutzerhandbuch.

- Wenn IE8 und neuere Versionen von Mozilla Firefox Release 3 verwendet werden, ignoriert der Browser vollständig die Antwort, die der SWA zurückgibt und maskiert sie mit seiner eigenen Fehlerseite. Dieses Browserverhalten läuft dem Zweck der 403-Benachrichtigung zuwider und verursacht eine Unterbrechung der Funktion.

Lösung

In diesem Abschnitt wird der Prozess beschrieben, der bei aktivierter HTTPS-Entschlüsselung auf dem SWA ausgeführt wird. Dieses Problem wurde in SWA Version 7.7.0-500 und höher behoben (Cisco Bug-ID CSCzv25138). Verwenden Sie zur Problemumgehung die bereitgestellten Informationen, um sicherzustellen, dass Ihr System entsprechend konfiguriert ist.

Das folgende Beispiel zeigt den Datenverkehrsfluss beim Senden einer expliziten HTTPS-Anforderung:

- Wenn die HTTPS-Entschlüsselung aktiviert ist, überprüft der SWA zuerst die Anforderung anhand der Entschlüsselungsrichtlinien.

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

- Wenn die Anforderung als ENTSCHLÜSSELT markiert ist, wird sie anhand der Zugriffsrichtlinien validiert. Wenn die Zugriffsrichtlinie in diesem Fall so konfiguriert ist, dass eine WARNUNG oder BLOCKIERUNG ausgelöst wird, wird die EUN-Seite richtig angezeigt. Leider muss der Benutzer zur Bestätigung zur HTTP-Seite und zur Bestätigung navigieren. Hierfür muss er über den Proxy und anschließend zur HTTPS-Site navigieren.

- Der SWA speichert die Client-IP-Adresse und benötigt erst nach Ablauf des Zeitgebers eine weitere Bestätigung.

Zugehörige Informationen

- Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD (Allgemeine Bereitstellung) - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.