

و Notification و WSA Warning تاحفص ضرعت ال ةحي رصلا HTTPS تابلطل حيحص لكشب EUN

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المشكلة](#)
- [الحل](#)

المقدمة

يصف هذا المستند مشكلة تتم مصادفتها على جهاز أمان الويب (WSA) من Cisco عندما لا تعرض صفحات التحذير أو الإقرار أو إعلام المستخدم النهائي (EUN) بشكل صحيح لطلبات HTTPS الصريحة. كما يتم توفير حل بديل لهذه المشكلة.

المتطلبات الأساسية

المتطلبات

تفترض المعلومات الواردة في هذا المستند أن:

- يتم نشر عناوين وكيل WSA في الوضع الصريح.
- تم حظر طلبات HTTPS أو تحذيرها أو مطالبتها بإشعار المستخدم.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco WSA.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المشكلة

لا تعرض صفحات التحذير أو الإقرار أو EUN بشكل صحيح لطلبات HTTPS الصريحة. يعرض المستعرض صفحة إعلام غير مكتملة، أو لا يعرض الصفحة على الإطلاق ويعرض صفحة خطأ بدلاً من ذلك.

هناك عدة مشاكل تحيط بهذه الصفحات عند استخدام طلبات HTTPS الصريحة. عند تكوين المستعرض لاستخدام وكيل، يتم توجيه حركة مرور بيانات HTTPS إلى WSA عبر HTTP. تم تنسيق هذا الطلب كـ HTTPS عبر HTTP.

هناك مشكلتان معروفتان بالمستعرضات التي لا تعالج ردود HTTP بشكل صحيح والتي يرجعها WSA لطلبات HTTPS الصريحة. عندما يكون طلب HTTPS الصريح إما محظورا، أو محذورا، أو يتطلب إقرارا من المستخدم، ترجع WSA رمز حالة 403. ضمن هذا الرد، يتضمن WSA محتوى الإعلام الذي يجب عرضه عادة على الشاشة حتى يمكن عرضه. ومع ذلك، في بعض الحالات، يتعذر على المستعرض فهم الرد ضمن المحتوى الذي تم إرجاعه. هذا هو سلوك المتصفح الذي تتم ملاحظته:

- عند استخدام Internet Explorer الإصدار 6 (IE6) وبعض إصدارات IE7، تفشل هذه الطلبات في تقديم المحتوى الكامل للرد على HTML. يقوم المستعرض بتكريم وحدات البايت القليلة الأولى فقط (المحتوى ضمن الحزمة الأولى) ويتجاهل الباقي. في مثل هذه الحالات، ترى صفحة غير مكتملة تعرض بضعة حروف فقط. ملاحظة: إذا كانت هذه هي الحالة، فإن Cisco توصيك بتقليص صفحة الإعلام الافتراضية من رد WSA. لمزيد من المعلومات حول كيفية تحرير صفحة EUN، ارجع إلى قسم تحرير صفحات إعلام منفذ IronPort في دليل مستخدم WSA.
- عند استخدام IE8 والإصدارات الأحدث من Mozilla Firefox الإصدار 3، يتجاهل المستعرض تماما الرد الذي تقوم WSA بإرجاعه ويقنعه باستخدام صفحة الأخطاء الخاصة به. يهزم سلوك المستعرض هذا الغرض من إعلام 403 ويتسبب في مقاطعة الميزة.

الحل

يصف هذا القسم العملية التي تحدث عند تمكين فك تشفير HTTPS على WSA. كحل بديل للمشكلة التي تم وصفها سابقا، أستخدم المعلومات المتوفرة لضمان تكوين النظام لديك وفقا لذلك.

فيما يلي مثال على تدفق حركة المرور عند إرسال طلب HTTPS صريح:

- عند تمكين فك تشفير HTTPS، يتحقق WSA أولا من صحة الطلب مقابل سياسات فك التشفير.
- إذا تم وضع علامة على الطلب للمرور، يتم السماح بحركة المرور بالمرور (بدون تحذير أو EUN).
- إذا تم تمييز الطلب على أنه تم فك تشفيره، فسيتم التحقق من صحة الطلب مقابل نهج Access. في هذه الحالة، إذا تم تكوين نهج الوصول من أجل التحذير أو الحظر، فسيتم عرض صفحة EUN بشكل صحيح. لسوء الحظ، للإقرار، يجب أن ينتقل المستخدم إلى صفحة HTTP و ACKNOWLEDGE، الأمر الذي يتطلب التنقل عبر الوكيل ثم إلى موقع HTTPS.
- يتذكر WSA عنوان IP الخاص بالعميل ولا يتطلب إقرارا آخر حتى تنتهي صلاحية المؤقت.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزلچنلإل دن تسمل