كيف تستجيب معرفات Cisco الآمنة لفيروس NIMDA

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
يحمي مستشعر مضيف Cisco IDS من NIMDA
يعرف مستشعر شبكة Cisco IDS NIMDA
الإجراءات الموصى بها
معلومات ذات صلة

المقدمة

يشرح هذا المستند كيفية تعريف "نظام اكتشاف الاقتحام الآمن (IDS) من Cisco" للخطر الذي يمكن أن يتعرض له خادم الويب ومنعه من الهجمات بواسطة دودة NIMDA (المعروفة أيضا باسم "فيروس المفهوم"). فالأعمال التقنية المعقدة للدودة تتجاوز نطاق هذه النشرة وتتم توثيقها جيدا في أماكن أخرى. يمكن العثور على أحد أفضل الأوصاف التقنية لدودة النيمدا في CERT® Advisory CA-2001-26 NIMDA Worm .

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

دودة النيمدا عبارة عن فيروس هجين ينتشر بقوة على الإنترنت. لفهم NIMDA وقدرات معرفات Cisco للحد من انتشارها، من المهم تحديد هذين المصطلحين:

- تشير **الدودة** إلى شفرة خبيثة تنتشر تلقائيا بدون تدخل بشري.
- يشير **الفيروس** إلى شفرة خبيثة تنتشر عبر نوع ما من التدخل البشري، مثل عندما تفتح رسالة بريد إلكتروني، أو تصفح موقع ويب مصاب، أو تنفيذ ملف مصاب يدويا.

فدودة النيمدا هي في الواقع هجين يظهر خصائص كل من الدودة والفيروس. ويصيب هذا المرض بعدة طرق، معظمها يتطلب تدخل الإنسان. يقوم مستشعر مضيف Cisco بحظر طرق العدوى الشبيهة بالفيروسات المتنقلة التي تنتشر عبر نقاط الضعف في Microsoft's Internet Information Server (IIS). لا تقوم معرفات Cisco بحظر طرق العدوى اليدوية الشبيهة بالفيروس، مثل عند فتح مرفق بريد إلكتروني أو إستعراض موقع ويب مصاب أو تنفيذ ملف مصاب يدويا.

يحمي مستشعر مضيف Cisco IDS من NIMDA

يمنع مستشعر مضيف Cisco IDS هجمات إجتياز الدليل، والتي تتضمن تلك المستخدمة من قبل دودة NIMDA. عندما تحاول الدودة أختراق خادم ويب محمي بمعرفات IDS من Cisco، يفشل الهجوم ولا يتم أختراق الخادم.

تمنع قواعد مستشعر مضيف Cisco هذه نجاح دودة NIMDA:

- إجتياز دليل IIS (القواعد الأربعة)
- تنفيذ التعليمات البرمجية وتجريب دليل IIS (أربعة قواعد)
- إجتياز دليل الترميز السداسي العشري المزدوج (أربعة قواعد) ل IIS

كما يدافع مستشعر مضيف Cisco IDS عن التغييرات غير المصرح بها على محتوى الويب، لذلك لا يسمح للدودة بتغيير صفحات الويب من أجل نشر نفسها إلى خوادم أخرى.

يتوافق نظام اكتشاف الاقتحام من Cisco مع أفضل ممارسات الأمان القياسية لحماية ملقمات الويب من NIMDA. وتملي أفضل الممارسات هذه عدم قراءة البريد الإلكتروني أو إستعراض الويب من خادم ويب للإنتاج، وكذلك عدم وجود مشاركات شبكة مفتوحة على خادم. يمنع مستشعر مضيف Cisco IDS خادم الويب من التعرض للخطر من خلال إستخدامات HTTP و IIS. وتضمن أفضل الممارسات المذكورة أعلاه عدم وصول دودة النمدا إلى خادم الويب بوسائل يدوية.

يعرف مستشعر شبكة Cisco IDS NIMDA

يحدد مستشعر شبكة Cisco IDS هجمات تطبيقات الويب، والتي تتضمن تلك المستخدمة من قبل دودة NIMDA. يمكن لمستشعر الشبكة تحديد الهجمات وتوفير تفاصيل حول الأجهزة المضيفة المتأثرة أو التي تم تعريضها للخطر لعزل عدوى النمسا.

يوجه مستشعر شبكة Cisco IDS هذا إطلاق النار:

- الوصول إلى (SigID 5081 WWW WinNT cmd.exe)
- فك الترميز المزدوج (SigID 5124 IIS CGI)
- هجوم (SigID 5114 WWW IIS Unicode)
- هجوم تنفيذ (SigID 3215 IIS dot)
- هجوم تحطم نقطة (SIGid 3216 IIS)

ولا يرى المشغلون إنذارا يحدد اسم نندا بالاسم. ويرون سلسلة من الإنذارات التي يشار إليها باسم "نيمدا"، وهي تحاول إستغلال مآرب مختلفة للإضرار بالهدف. تحدد التنبيهات عنوان المصدر للأجهزة المضيفة التي تم إختراقها والتي يجب عزلها عن الشبكة وتنظيفها وترقيتها.

الإجراءات الموصى بها

اتبع الخطوات التالية للحماية من دودة النمدا:

1. تطبيق آخر التحديثات ل Microsoft Outlook و Outlook Express و Internet Explorer و IIS المتوفرة من Microsoft .
2. قم بتحديث برنامج فحص الفيروسات لديك باستخدام أحدث حزمة لتخفيف انتشار الفيروس.**ملاحظة:** يمكنك تنزيل أحدث حزمة فيروسات لحماية الكمبيوتر من الإصابة. إذا كان الكمبيوتر الشخصي قد تعرض للإصابة بالفعل، فإن برنامج مكافحة الفيروسات هذا يتيح لك فحص محرك الأقراص الثابتة لجهاز الكمبيوتر الخاص بك يدويا وتنظيف هذه العدوى من الجهاز.
3. قم بنشر معرفات Cisco للحد من التهديد، واحتواء العدوى، وحماية الخوادم.

معلومات ذات صلة

- كيفية حماية شبكتك من فيروس NIMDA
- إشعارات وتوجيهات أمان المنتج من Cisco
- صفحة دعم اكتشاف التسلل الآمن من Cisco
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).