إستخدام توقيعات مطابقة السلسلة المخصصة ل Cisco Secure IDS/NetRanger ل دعد تجاوز سعة التخزين المؤقت عن "رمز أحمر" Microsoft Index مداخ ISAPI قلحم في ةدودلل IIS 4.0 و 5.0 في

المحتويات

المقدمة

وحتى نهاية تموز (يوليو) 2003، قدرت منظمة أبحاث مستقلة في كارلسباد، كاليفورنيا، ان دودة "الشفرة الحمراء" كلفت الشركات 1،2 بليون دولار (اميركي) في الشفاء من ضرر الشبكة والإنتاجية المفقودة. وقد ارتفع هذا التقدير بشكل كبير مع الإصدار اللاحق للدودة "الشفرة الحمراء الثانية" الأكثر قوة. أثبت نظام اكتشاف الاقتحام الآمن (IDS) من Cisco، وهو مكون أساسي في مخطط Cisco الآمن، قيمته في اكتشاف مخاطر أمان الشبكة والتخفيف منها، بما في ذلك دودة "الرمز الأحمر".

يصف هذا المستند تحديث برنامج للكشف عن طريقة الاستغلال المستخدمة من قبل دودة "الشفرة الحمراء" (راجع التوقيع 2 أدناه).

يمكنك إنشاء توقيعات مطابقة السلسلة المخصصة الموضحة أدناه لتعقب إستغلال تجاوز سعة التخزين المؤقت لخوادم الويب التي تشغل Microsoft Windows NT و 4.0 Internet Information Services (IIS) أو Windows 2000 و IIS 5.0. لاحظ أيضا أن خدمة الفهرسة في الإصدار بيتا من Windows XP معرضة أيضا للخطر. تتوفر نصيحة الأمان التي تصف هذه الثغرات الأمنية على http://www.eeye.com/html/Research/Advisories/AD20010618.html . قامت Microsoft بإصدار حزمة تصحيح لهذه الثغرة التي يمكن تنزيلها من http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx .

أصبحت التوقيعات التي تمت مناقشتها في هذا المستند متوفرة في تحديث التوقيع الإصدار S(5). توصي Cisco Systems بترقية أجهزة الاستشعار إلى 2.2.1.8 أو S3(1)2.5 تحديث توقيع قبل تنفيذ هذا التوقيع. يمكن للمستخدمين المسجلين تنزيل تحديثات التوقيع هذه من مركز برامج الأمان من Cisco. يمكن لجميع المستخدمين الاتصال بدعم Cisco التقني عبر البريد الإلكتروني والهاتف من خلال جهات اتصال Cisco في جميع أنحاء العالم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- Microsoft Windows NT و IIS 4.0
- Microsoft Windows 2000 و IIS 5.0

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.

الاصطلاحات

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

توقيعات مطابقة السلسلة المخصصة

هناك توقيعان مخصصان لمطابقة السلسلة لمعالجة هذه المشكلة. يتم وصف كل توقيع أدناه، كما يتم توفير إعدادات المنتج القابلة للتطبيق.

التوقيع 1 — وصول خادم الفهرس مع محاولة الاستغلال

يتم تشغيل هذا التوقيع على محاولة تجاوز سعة التخزين المؤقت على ملحق ISAPI الخاص ب Indexing Server بالاقتران مع محاولة تمرير رمز shell إلى الخادم للحصول على حق الوصول المميز في النموذج الأصلي للرمز. يتم تشغيل التوقيع فقط على محاولة تمرير رمز shell إلى الخدمة الهدف في محاولة للحصول على وصول كامل على مستوى النظام. إحدى المشاكل المحتملة هي أن هذا التوقيع لا يتم تشغيله إذا لم يحاول المهاجم تمرير أي رمز من رموز Shell، ولكن يقوم فقط بتشغيل تجاوز سعة التخزين المؤقت مقابل الخدمة في محاولة لتحطيم IIS وإنشاء رفض الخدمة.

السلسلة

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

إعدادات المنتج

- التكرارات: 1
- المنفذ: 80

ملاحظة: إذا كان لديك خوادم ويب تنصت إلى منافذ TCP الأخرى (على سبيل المثال، 8080)، فأنت بحاجة إلى إنشاء مطابقة سلسلة مخصصة منفصلة لكل رقم منفذ.

- مستوى خطورة التنبيه الموصى به:عالي (5)Cisco Secure Policy Manager (مدير UNIX)
- الإتجاه: إلى

SIGNATURE 2 — تجاوز سعة التخزين المؤقت للوصول إلى خادم الفهرس ل ""Code Red WORM

يعمل التوقيع الثاني على محاولة تجاوز سعة التخزين المؤقت على ملحق ISAPI الخاص ب Indexing Server بالاقتران مع محاولة تمرير رمز shell إلى الخادم للحصول على حق الوصول المميز في النموذج الغامض الذي تستخدمه الدودة "Code Red". يتم تشغيل هذا التوقيع فقط عند محاولة تمرير رمز shell إلى الخدمة الهدف في محاولة للحصول على الوصول الكامل على مستوى النظام. إحدى المشاكل المحتملة هي أن هذا التوقيع لا يتم تشغيله إذا لم يحاول المهاجم تمرير أي رمز من رموز Shell، ولكن يقوم فقط بتشغيل تجاوز سعة التخزين المؤقت مقابل الخدمة في محاولة لتحطيم IIS وإنشاء رفض الخدمة.

السلسلة

```
default[.]ida[?][a-zA-Z0-9]+%u[/]
```

ملاحظة: لا توجد مسافات فارغة في السلسلة أعلاه.

إعدادات المنتج

- التكرارات: 1
- المنفذ: 80

ملاحظة: إذا كان لديك خوادم ويب تنصت إلى منافذ TCP الأخرى (على سبيل المثال، 8080)، فأنت بحاجة إلى إنشاء مطابقة سلسلة مخصصة منفصلة لكل رقم منفذ.

- مستوى خطورة التنبيه الموصى به:عالي (5)Cisco Secure Policy Manager (مدير UNIX)
- الإتجاه: إلى

لمزيد من المعلومات حول معرفات Cisco الآمنة، ارجع إلى اكتشاف التسلل الآمن من Cisco.

معلومات ذات صلة

- الدعم التقني - الموجهات
- إستشارات الأمان 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).