الحماية ضد هجمات منفذ UDP التشخيصي لمنع الخدمة

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
وصف المشكلة
هجوم منفذ تشخيص UDP
الدفاع ضد الهجمات المباشرة الموجهة إلى أجهزة الشبكة
تعطيل منافذ تشخيص UDP
منع الشبكة من إستضافة هجوم دون قصد
منع إرسال عناوين IP غير الصالحة
منع إستلام عناوين IP غير الصالحة
الملحق: وصف الخوادم الصغيرة
معلومات ذات صلة

المقدمة

هناك هجوم محتمل على مزودي خدمة الإنترنت (ISPs) يستهدف أجهزة الشبكة.

- **هجوم المنفذ التشخيصي لبروتوكول مخطط بيانات المستخدم (UDP)**:يرسل المرسل وحدة تخزين من الطلبات لخدمات تشخيص UDP على الموجه. وهذا يتسبب في إستهلاك جميع موارد وحدة المعالجة المركزية (CPU) لخدمة الطلبات المزيفة.

يصف هذا المستند كيفية حدوث هجوم منفذ UDP التشخيصي المحتمل ويقترح طرق الاستخدام مع برنامج Cisco IOS®للدفاع ضده.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة. تتوفر بعض الأوامر المشار إليها في هذا المستند فقط بدءا من الإصدار 10.2(9) من برنامج Cisco IOS Software، و 10.3(7)، و 11.0(2)، وجميع الإصدارات التالية. هذا أمر التقصير في cisco ios برمجية إطلاق 12.0 وفيما بعد.

الاصطلاحات

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

وصف المشكلة

هجوم منفذ تشخيص UDP

بشكل افتراضي، يحتوي موجه Cisco على سلسلة من المنافذ التشخيصية التي تم تمكينها لبعض خدمات UDP و TCP. وتتضمن هذه الخدمات الارتداد والتشكيل والتجاهل. عندما يقوم مضيف بإرفاق هذه المنافذ، يتم إستهلاك مقدار صغير من سعة وحدة المعالجة المركزية (CPU) لخدمة هذه الطلبات.

إذا قام جهاز هجومي واحد بإرسال وابل كبير من الطلبات باستخدام عناوين IP مختلفة وعشوائية ومزيفة للمصدر، من الممكن أن يصبح الموجه من Cisco مغلوطا ويبطئ أو يفشل.

تتضمن المظاهر الخارجية للمشكلة رسالة خطأ كاملة لجدول العملية (SYS-3 NOPROC) أو إستخدام عال جدا لوحدة المعالجة المركزية. يعرض أمر **show process** EXEC الكثير من العمليات التي لها نفس الاسم، مثل "صدى UDP".

الدفاع ضد الهجمات المباشرة الموجهة إلى أجهزة الشبكة

تعطيل منافذ تشخيص UDP

يجب حماية أي جهاز شبكة يحتوي على خدمات UDP و TCP التشخيصية بواسطة جدار حماية أو تعطيل الخدمات. بالنسبة لموجه Cisco، يمكن تحقيق ذلك باستخدام أوامر التكوين العام هذه.

```
no service udp-small-servers
no service tcp-small-servers
```

راجع الملحق للحصول على مزيد من المعلومات حول هذه الأوامر. تتوفر الأوامر بدءا من برنامج Cisco IOS الإصدار 10.2(9) و 10.3(7) و 11.0(2) وجميع الإصدارات التالية. هذا أمر التقصير في cisco ios برمجية إطلاق 12.0 وفيما بعد.

منع الشبكة من إستضافة هجوم دون قصد

بما أن الآلية الأساسية لهجمات رفض الخدمة هي إنشاء حركة المرور المستمدة من عناوين IP العشوائية، توصي Cisco بتصفية حركة المرور الموجهة إلى الإنترنت. والمفهوم الأساسي هو التخلص من الحزم ذات عناوين IP للمصدر غير الصالحة أثناء دخولها إلى الإنترنت. لا يمنع هذا هجوم رفض الخدمة على شبكتك. إلا أنه يساعد الأطراف المهاجمة على إستبعاد موقعك كمصدر للمهاجم. بالإضافة إلى ذلك، فإنها تمنع إستخدام شبكتك لهذه الفئة من الهجمات.

منع إرسال عناوين IP غير الصالحة

بتصفية الحزم على الموجهات التي تصل شبكتك بالإنترنت، يمكنك السماح فقط للحزم ذات عناوين IP المصدر الصالحة بمغادرة شبكتك والوصول إلى الإنترنت.

على سبيل المثال، إذا كانت شبكتك تتكون من الشبكة 172.16.0.0، وكان الموجه الخاص بك يتصل ب ISP باستخدام واجهة FDDI0/1، فيمكنك تطبيق قائمة الوصول مثل هذا:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log [1]

interface Fddi 0/1
ip access-group 111 out
```

[1]يحدد السطر الأخير من قائمة الوصول ما إذا كانت هناك أي حركة مرور بعنوان مصدر غير صالح يدخل الإنترنت. يساعد ذلك في تحديد مصدر الهجمات المحتملة.

منع إستلام عناوين IP غير الصالحة

بالنسبة إلى موفري خدمات الإنترنت (ISPs) الذين يقدمون الخدمة إلى الشبكات الطرفية، توصي Cisco بشدة بالتحقق من صحة الحزم الواردة من عملائك. ويمكن تحقيق ذلك باستخدام عوامل تصفية الحزم الواردة على موجهات الحدود.

على سبيل المثال، إذا كان لدى عملائك أرقام الشبكة هذه متصلة بالموجه الخاص بك من خلال واجهة FDDI المسماة "FDDI 1/0"، فيمكنك إنشاء قائمة الوصول هذه.

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface Fddi 1/0
ip access-group 111 in
```

ملاحظة: يحدد السطر الأخير من قائمة الوصول ما إذا كانت هناك أي حركة مرور بعنوان مصدر غير صالح يدخل الإنترنت. يساعد ذلك في تحديد موقع مصدر الهجوم المحتمل.

الملحق: وصف الخوادم الصغيرة

الخوادم الصغيرة هي خوادم (للخوادم النصلية، في رمز UNIX) يتم تشغيلها في الموجه والتي تكون مفيدة للتشخيص. لذلك، فهي تعمل بشكل افتراضي.

أوامر خوادم TCP و UDP الصغيرة هي:

- **service tcp-small-servers**
- **خدمة UDP-small-servers**

إذا لم تكن ترغب في أن يوفر الموجه لديك أي خدمات غير متعلقة بالتوجيه، فقم بإيقاف تشغيلها (باستخدام الصيغة **no** من الأوامر السابقة).

خوادم TCP الصغيرة هي:

- **الصدى** — أصداء ما تكتبون. اكتب الأمر **telnet x.x.x.x echo** لترى.
- **Chargen** — يولد تدفقا من بيانات ASCII. اكتب الأمر **telnet x.x.x.x chargen** لرؤيته.
- **تجاهل** — يرمي كل ما تكتبه بعيدا. اكتب الأمر **telnet x.x.x.x discard** لترى.
- **daytime**—إرجاع تاريخ ووقت النظام، إذا كان ذلك صحيحا. هذا صحيح إذا قمت بتشغيل NTP أو قمت بتعيين التاريخ والوقت يدويا من مستوى EXEC. اكتب الأمر **telnet x.x.x.x daytime** لترى.

خوادم UDP الصغيرة هي:

- **echo**—يردد حمولة مخطط البيانات الذي تقوم بإرساله.
- **discard**— يعرض مخطط البيانات الذي تقوم بإرساله في صمت.
- **chargen**—يعرض مخطط البيانات الذي ترسله وتستجيب له بسلسلة من 72 حرفا من حروف ASCII يتم إنهاؤها باستخدام CR+LF.

ملاحظة: تدعم جميع مربعات UNIX تقريبا الخوادم الصغيرة المذكورة سابقا. كما يوفر الموجه خدمة Finger وخدمة تمهيد تشغيل الخط غير المتزامنة. يمكن إيقاف تشغيل هذه العناصر بشكل مستقل باستخدام أوامر التكوين العامة **no service finger** و**no ip bootp server**، على التوالي.

معلومات ذات صلة

- برنامج IOS 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).