

-----  
UNAM-CERT

Departamento de Seguridad en Computo

DGSCA- UNAM

Nota de Seguridad UNAM-CERT 2006-001

DNS Amplification Attack  
-----

Los servidores de nombres de dominio pueden ser usados para llevar a cabo ataques de negación de servicio a causa de errores en la configuración en el nivel de recursión que permiten

Fecha de Liberación: 7 de Marzo de 2006

Ultima Revisión: 14 de Marzo de 2006

Fuente: UNAM-CERT y diversos Grupos de Seguridad

Riesgo

-----  
Crítico

Problema de Vulnerabilidad

-----  
Remoto

Tipo de Vulnerabilidad

-----  
Negación de servicio

I. Descripción

=====

En un servidor DNS que permita consultas recursivas sin verificación, un atacante puede enviar una gran cantidad de peticiones con una dirección IP falsificada (spoof), el DNS procesa estas peticiones como válidas mandando una respuesta al sistema al cual se quiere atacar y al ser de un tamaño mayor las respuestas del DNS que sus peticiones, pueden inundar el sistema atacado de respuestas de DNS.

II. Impacto

=====

Un servidor vulnerable puede sufrir una negación de servicio y/ o provocar una negación de servicio en el sistema víctima del ataque en base a la gran cantidad de respuestas que genere.

III. Solución

=====

Configurar los servidores DNS de tal manera que sólo se permitan las consultas recursivas a una cantidad limitada de hosts a los que se tiene confianza o, en el caso de ser un DNS que no tiene ningún dominio al cual permitirle consultas recursivas, bloquear la recursión por completo.

A continuación se proveen algunos ejemplos de configuración donde se elimina o se limita la recursión.

En el caso de ser un servidor BIND 8/9 el cual no tiene ningún dominio de menor jerarquía al cual tengamos estrictamente que permitirle realizar consultas recursivas se realizaría lo siguiente en el archivo de configuración de BIND :

```
options {  
  directory "/var/named";  
  recursion no;
```

};

En el caso de Microsoft DNS se haría añadiendo un registro de tipo REG\_DWORD llamado NoRecursion con el valor 1 a la siguiente llave del registro  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

El siguiente ejemplo es útil en el caso en que tengamos dominios de menor jerarquía a los cuales tengamos que permitirles la recursión siempre y cuando esos hosts sean de nuestra confianza. Para BIND 8/9 se realizaría de la siguiente manera:  
acl recurseallow { x.x.x.x; y.y.y.y; z.z.z.z; };  
options {  
directory "/var/named";  
allow-recursion { recurseallow; };  
};

En el caso de Microsoft DNS la modificación sería la siguiente:  
En la consola de administración de DNS, dar click derecho en el objeto DNS e ir a Propiedades Click en Forwarders tab, habilitar la check box Enable forwarders e incluir en la caja de texto las ips de las cuales aceptamos recursión

#### IV. Apéndice A. Referencias

=====

[http://www.cert.org/incident\\_notes/IN-2000-04.html](http://www.cert.org/incident_notes/IN-2000-04.html)  
[http://www.us-cert.gov/reading\\_room/DNS-recursion121605.pdf](http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf)  
[http://news.com.com/Old+software+weakening+Nets+backbone.+survey+says/2100-7347\\_3-5913771.html](http://news.com.com/Old+software+weakening+Nets+backbone.+survey+says/2100-7347_3-5913771.html)  
<http://www.netadmintools.com/art234.html>

-----  
El Departamento de Seguridad en Cómputo/UNAM-CERT agradece el apoyo en la elaboración, revisión y traducción de éste boletín a:

- \* Ruben Aquino Luna (raqino at seguridad dot unam dot mx)
- \* Juan Carlos Guel Lopez (cguel at seguridad dot unam dot mx)
- \* Edson Vieyra (evieyra at seguridad dot unam dot mx)

#### INFORMACIÓN

=====

Éste documento se encuentra disponible en su formato original en la siguiente dirección:

Español:

- \* Nota de Seguridad UNAM-CERT-2006-001

<http://www.cert.org.mx/nota/?vulne=5077>

- \* Documento que describe DNS Amplification Attack

<http://www.seguridad.unam.mx/labsec/tuto/?id=181&ap=tutorial&cabecera=2>

Mas informacion:

UNAM-CERT  
Equipo de Respuesta a Incidentes UNAM  
Departamento de Seguridad en Cómputo  
E-Mail: seguridad@seguridad.unam.mx  
<http://www.cert.org.mx>  
<http://www.seguridad.unam.mx>  
ftp://ftp.seguridad.unam.mx  
Tel: 56 22 81 69