UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−018

Múltiples implementaciones de DNS vulnerables a ataque de cache poisoning

---

Deficiencias en el protocolo DNS e implementaciones comunes de DNS facilitan un ataque “DNS cache poisoning”. Se han demostrado técnicas efectivas para atacar estas vulnerabilidades.

Fecha de Liberación: 8 de Julio de 2008

Ultima Revisión: 8 de Agosto de 2008

Fuente: US−CERT

CVE ID: **CVE−2008−1447**

Problema de Vulnerabilidad

Remoto

I. Sistemas Afectados

Los sistemas que implementan:

- Caching DNS resolvers
- DNS stub resolvers

Los sistemas afectados incluyen tanto clientes como servidores y cualquier otro otro sistema en red que incluya esta funcionalidad.

II. Descripción

DNS cache poisoning (algunas veces nombrado como cache pollution) es una técnica de ataque que permite a un intruso insertar datos DNS falsos en el cache de un servidor de nombres. El concepto general se conoce desde hace tiempo, y una serie de deficiencias inherentes en el protocolo DNS y defectos en implementaciones de DNS comunes que facilitan el cache poisoning han sido previamente identificados y descritos en la literatura pública. Ejemplos de estas vulnerabilidades se pueden encontrar en la nota de seguridad identificada con el número VU#800113.

Recientes investigaciones sobre esta y otras vulnerabilidades relacionadas han producido métodos de explotación extremadamente efectivos para lograr un cache poisoning. Se han desarrollado herramientas y técnicas que pueden

envenenar un dominio que el intruso haya escogido en la mayoría de las implementaciones actuales. Como resultado, el consenso de implementadores de software DNS ha considerado añadir un método para que el puerto origen sea asignado de forma aleatoria en el DNS.

El US−CERT da seguimiento a esta vulnerabilidad con el identificador VU#800113. Este número de referencia corresponde a CVE−2008−1447.

III. Impacto

Un intruso con la habilidad para lanzar exitosamente un ataque “cache poisonig” puede lograr que los clientes de un servidor de nombres sean redirigidos hacia sitos erróneos y posiblemente maliciosos o hacia sitios especialmente modificados en ciertos servicios. En consecuencia, el tráfico web, correo electrónico y otros datos importantes de la red pueden ser redirigidos hacia sistemas controlados por un intruso.

IV. Solución

Se han liberado una serie de actualizaciones por parte de la mayoría de los proveedores para aplicar métodos en el que la asignación del puerto para el servidor de nombres sea de forma aleatoria. Este cambio reduce significativamente la posibilidad de ataques “DNS cache poisoning”. Para más información, se encuentra disponible la nota sobre la vulnerabilidad identificada como VU#800113.

Como se mencionó, los “Stub resolvers” también son vulnerables a estos ataques. Un “Stub resolver” que pueda hacer consultas como respuesta a un ataque y en consecuencia recibir paquetes del intruso, debe ser actualizado para corregir el problema. Los administradores de sistemas deberán estar atentos a las actualizaciones de sus proveedores que agreguen la funcionalidad de asignación aleatoria del puerto.

Workarounds

Restricción de acceso

Los administradores, particularmente los que no puedan aplicar una actualización, podrán mitigar la exposición a esta vulnerabilidad mediante la restricción de fuentes que puedan solicitar la recursividad de consultas DNS. Es importante tener en cuenta que la restricción de acceso, todavía permite a los usuarios con acceso explotar esta vulnerabilidad.

Filtrado de paquetes en el perímetro de red

Debido a que se requiere hacer spoofing de direcciones IP, es necesario tomar medidas en el perímetro para detener estos ataques. Los administradores deberán ser cuidadosos a la hora de filtrar las direcciones IP en el perímetro de red. Las mejores practicas para mitigar este tipo de problemas se describen en RFC 2827, RFC 3704, RFC 3013. Es importante entender la infraestructura de red antes de hacer algún cambio.

Ejecutar un DNS cache local

En lugar de implementar métodos en los que el puerto sea asignado de forma aleatoria en cada equipo, existe la posibilidad de implementar un DNS que funcione de forma local que ayude en la resolución de nombres. Este servicio, debido a que estará en un ambiente controlado, podrá ser utilizado por todos clientes y servidores que, de acuerdo a la topología, estén dentro de la red. Esto debe hacerse en conjunto con la segmentación de red y estrategias de filtrado de paquetes mencionadas previamente.

Inhabilitar la recursividad

Inhabilitar la recursividad en los servidores de nombres que respondan a solicitudes DNS realizadas por sistemas no confiables.

Aplicar métodos para asignar puertos de forma aleatoria

Los proveedores que implementan software DNS deben revisar el documento del IETF conocido como "Measures for making DNS more resilient against forged answers", este documento brinda información adicional sobre estrategias e implementaciones que ayudan a mitigar este tipo de problemas.

Este documento es un trabajo en progreso que puede ser modificado antes de su publicación como un RFC.

V. Referencias

- US−CERT Vulnerability Note VU#800113 − <http://www.kb.cert.org/vuls/id/800113>
- US−CERT Vulnerability Note VU#484649 − <http://www.kb.cert.org/vuls/id/484649>
- US−CERT Vulnerability Note VU#252735 − <http://www.kb.cert.org/vuls/id/252735>
- US−CERT Vulnerability Note VU#927905 − <http://www.kb.cert.org/vuls/id/927905>
- US−CERT Vulnerability Note VU#457875 − <http://www.kb.cert.org/vuls/id/457875>
- Internet Draft: Measures for making DNS more resilient against forged answers − <http://tools.ietf.org/html/draft−ietf−dnsext−forgery−resilience>
- RFC 3833 − <http://tools.ietf.org/html/rfc3833>
- RFC 2827 − <http://tools.ietf.org/html/rfc2827>
- RFC 3704 − <http://tools.ietf.org/html/rfc3704>
- RFC 3013 − <http://tools.ietf.org/html/rfc3013>
- Microsoft Security Bulletin MS08−037 − <http://www.microsoft.com/technet/security/bulletin/ms08−037.mspx>
- Internet Systems Consortium BIND Vulnerabilities − <http://www.isc.org/sw/bind/bind−security.php>

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Eduardo González Martínez (egonzalez at seguridad dot unam dot mx)
- Eduardo Espina García (eespina at seguridad dot unam dot mx)

- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- Israel Becerril Sierra (ibecerril at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47