PRESIDENCIA DEL CONSEJO DE MINISTROS

Oficina Nacional de GOBIERNO ELECTRÓNICO e INFORMÁTICA

BOLETIN DE SEGURIDAD DE LA INFORMACIÓN

Centro de Consulta e Investigación sobre Seguridad de la Información

Edición Nº 70/ 26 de Mayo de 2008

Visite el Portal del Estado Peruano: www.peru.gob.pe

CONTENIDO

FUENTES

- Hispasec
- Security Focus
- IBM
- Info Security
- Java
- VSAntivirus

VULNERABILIDAD EN FOXIT READER 2.3

Foxit Reader es un lector gratuito de archivos con formato PDF (Portable Document Format) que corre bajo distintas versiones de Linux y Windows Foxit Reader se está haciendo popular como alternativa a Adobe Reader, principalmente por su pequeño tamaño (2.55MB) en comparación con los 22.7MB que ocupa la última versión de Adobe Reader en Español.

La vulnerabilidad está causada por un error de límites en la función JavaScript util.printf(), al procesar el formato de cadenas que contengan un especificador de coma flotante. Esto podría ser aprovechado para causar un desbordamiento de búfer basado en pila por medio de un archivo PDF especialmente manipulado.

El error afecta a la última versión disponible de Foxit Reader, la 2.3 build 2825 y podría afectar a otras versiones anteriores incluso si no utilizan el plug-in de JavaScript.

MÁS INFORMACIÓN:

- **Foxit Reader 'util.printf()' Remote Buffer Overflow Vulnerability**
  http://www.securityfocus.com/bid/29288

VULNERABILIDAD EN SNORT

Snort es uno de los IDS (Sistema de Detección de Intrusiones) más extendidos. Distribuido de forma gratuita como Open Source, Snort puede detectar muchos de los patrones de ataque conocidos basándose en el análisis de los paquetes de red según unas bases de datos de firmas, además de reglas genéricas. Habitualmente la función de estos detectores es la de alertar sobre actividades sospechosas a través de cualquier mecanismo, aunque en ocasiones puede usarse para lanzar medidas destinadas a mitigar de forma automática el posible problema descubierto por el sensor.

El fallo reside en el reensamblado de paquetes IP fragmentados. Cuando Snort recibe paquetes fragmentados compara sus valores TTL. Snort tiene un valor predefinido para la diferencia de valores TTL entre paquetes, si el valor de la diferencia entre el primero de ellos y el resto es mayor que este valor los descartará y no aplicará ningún filtro o examen sobre ellos. Un atacante remoto podría aprovechar este fallo para saltar restricciones de seguridad modificando los valores TTL de los paquetes IP.

El problema se ha confirmado en Snort 2.8 y 2.6. El fallo queda corregido en la versión 2.8.1 disponible en el repositorio:
cvs.snort.org

MÁS INFORMACIÓN:

- **Multiple Vendor Snort IP Fragment TTL Evasion Vulnerability**
  http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=701

ACTUALIZACIONES DE SUN JAVA 6 UPDATE 6

Sun ha publicado una actualización a su producto Java (Java 6 Update 6), la cuál corrige al menos 13 vulnerabilidades y fallos. Dos de las mismas están consideradas de nivel alto (1), la máxima categoría de riesgo según la compañía.

Otras 3 vulnerabilidades están clasificadas con un nivel de riesgo (nivel 2), 6 fallos son considerados moderados (nivel 3), uno de nivel bajo (4), y de uno de ellos no se dan detalles, aunque se debe a la falta de un paquete de la instalación en versiones anteriores.

Los problemas con nivel de riesgo más alto (1), estan relacionados con la asignación de la memoria disponible para los programas en Windows Vista que afecta a algunos applets, y un excesivo consumo de memoria en Java Web Start 6.

Para comprobar si tiene instalada la última versión de Java, puede dirigirse al siguiente enlace:

http://java.com/es/download/installed.jsp

Desde allí mismo se recomendará el enlace para descargar e instalar la versión más reciente de Sun Java. También puede hacer ello desde el siguiente enlace:

http://java.com/es/

MÁS INFORMACIÓN:

- **Update Release Notes**
  http://java.sun.com/javase/6/webnotes/ReleaseNotes.htm
- **Java**
  http://java.com/es/
- **VSAntivirus**
  http://www.vsantivirus.com/vul-sunjava-200508.htm

VULNERABILIDAD EN IBM LOTUS DOMINO 6.X, 7.X Y 8.X

Se han corregido dos vulnerabilidades en IBM Lotus Domino (versiones 6, 7 y 8) que podrían permitir a un atacante remoto ejecutar código arbitrario.

- Se ha corregido un fallo cuando se procesan cabeceras de peticiones HTTP con el campo 'Accept-Language' excesivamente grande que podrían ocasionar un desbordamiento de la memoria intermedia basada en pila. Un atacante remoto podría ejecutar código arbitrario a través de peticiones HTTP especialmente manipuladas.

- Se ha corregido un fallo en el motor de servlets y contenedor de aplicaciones web al procesar entradas de datos no especificadas que no son correctamente filtradas. Un atacante remoto podría ejecutar código HTML y script arbitrarios en el contexto de la sesión del navegador de un usuario.

Se recomienda actualizar a las versiones 7.0.3 Fix Pack 1 (FP1) o 8.0.1 desde:

http://www.ibm.com/software/lotus/support/upgradecentral/index.html

MÁS INFORMACIÓN:

- **Lotus Domino Web server 'Accept-Language' stack overflow**
  http://www-1.ibm.com/support/docview.wss?uid=swg21303057
- **Potential vulnerability in servlet engine/Web container in Lotus Domino Web servers**
  http://www-1.ibm.com/support/docview.wss?uid=swg21303296
- **IBM Lotus Domino "Accept-Language" Stack Overflow**
  http://www.mwrinfosecurity.com/publications/mwri_ibm-lotus-domino-accept-language-stack-overflow_2008-05-20.pdf

CONGRESOS Y SEMINARIOS DEL 2008
Mayo 27 al 29 de 2008 **IV Congreso Internacional de Seguridad Electronica (Brasil)** http://www.abese.org.br/cis2008/
Junio 18 al 20 de 2008: **VIII Jornada Nacional de Seguridad Informática ACIS 2008 (Bogotá - Colombia)** http://www.acis.org.co/index.php?id=1066
Junio 23 al 25 de 2008: **The 5th International Conference on Autonomic and Trusted Computing (Oslo - Noruega)** http://www.ux.uis.no/atc08/
Junio 25 al 27 de 2008: **Sexto Congreso Collaborative Electronic Communications and eCommerce Technology and Research CollECTeR Iberoamérica 2008 (Madrid - España)** http://www.collecter.euitt.upm.es/
Julio 9 al 11 de 2008: **XIV Jornadas de Enseñanza Universitaria de la Informática (Granada - España)** http://jenui2008.ugr.es/
Septiembre 2 al 5 de 2008: **X Reunión Española de Criptología y Seguridad de la Información RECSI 2008 (Salamanca - España)** http://www.usal.es/~xrecsi/
Septiembre 10 al 12 de 2008: **EATIS 2008 Euro American Conference on Telematics and Information Systems (Aracajú - Brasil)** http://eatis.org/eatis2008/

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106