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 66/ 25 de Enero de 2008

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

CONTENIDO

FUENTES

- Securityfocus
- us-cert.gov
- Hispasec

VULNERABILIDADES EN ARCHIVOS FLASH

Se han reportado vulnerabilidades críticas en muchas de las herramientas web más populares que generan archivos Shockwave Flash (SWF), de forma automática, esto es Adobe, Dreamweaver, Adobe Acrobat, Connect (Macromedia Breeze), InfoSoft FusionCharts, y Techsmith Camtasia.

Los fallos hacen que los sitios web que albergan estos archivos SWF, sean vulnerables a ataques del tipo Cross-Site Scripting (XSS).

Las vulnerabilidades están relacionadas con el uso de ActionScript, el lenguaje utilizado para el desarrollo de las herramientas de autor. ActionScript permite el desarrollo de interfaces de usuario y aplicaciones, y no solo animaciones con Flash.

Los archivos vulnerables pueden ser utilizados por atacantes para ejecutar código JavaScript malicioso en el ámbito del sitio web que hospede estos archivos.

Se recomienda a los usuarios, actualizar las versiones de sus reproductores y plugins de Flash (Flash Player, etc.), a las versiones más recientes.

MÁS INFORMACIÓN:

- **XSS Vulnerabilities in Common Shockwave Flash Files**
  http://docs.google.com/View?docid=ajfxntc4dmsq_14dt57ssdw

VULNERABILIDADES EN ROUTERS ZYXEL P-330W

Se han encontrado varias vulnerabilidades en los routers ZyXEL P-330W que podrían ser aprovechado por atacantes para perpetrar ataques de cross-site scripting y peticiones falsas.

Se ha detectado que la interfaz de administración web del dispositivo se ve afectada por los siguientes problemas:

- La entrada pasada al parámetro "pngstr" en ping.asp no es debidamente saneada antes de ser devuelta al usuario.
- Varias vulnerabilidades en el dispositivo, que permite a usuarios realizar acciones a través de peticiones HTTP sin validar la identidad del usuario ni las peticiones. Esto puede ser aprovechado para cambiar la contraseña del administrador.

Se recomienda no navegar por otras páginas mientras se está dentro de la interfaz web de administración del dispositivo.

MÁS INFORMACIÓN:

- **[Full-disclosure] Ho Ho H0-Day - ZyXEL P-330W multiple XSS and XSRF vulnerabilities**
  http://lists.grok.org.uk/pipermail/full-disclosure/2007-December/059295.html

VULNERABILIDAD EN REALPLAYER 11

RealPlayer es empleado por millones de usuarios de Internet para reproducir archivos multimedia tanto de audio como de vídeo.

La vulnerabilidad hallada en RealPlayer 11 podría ser aprovechada por un atacante remoto para causar una denegación de servicio o ejecutar código arbitrario con los permisos de un usuario ejecutando la aplicación en un sistema vulnerable.

El problema está causado por un desbordamiento de búfer no especificado que se produce debido a un fallo en la comprobación de los límites de algunos datos de entrada introducidos por un usuario, antes de que sean copiados a un búfer demasiado pequeño. Esto podría ser aprovechado por un atacante remoto para causar una denegación de servicio o ejecutar código arbitrario si un usuario abre un archivo especialmente manipulado con una versión vulnerable de RealPlayer.

MÁS INFORMACIÓN:

- **RealPlayer 11 Unspecified Buffer Overflow Vulnerability**
  http://www.securityfocus.com/bid/27091/info
- **0day RealPlayer 11 exploit Demo**
  http://gleg.net/realplayer11.html
- **US-CERT Current Activity: Publicly Available Exploit Code for RealPlayer**
  http://www.us-cert.gov/current/index.html#public_exploit_code_for_realplayer

CONGRESOS Y SEMINARIOS DEL 2008
Enero 22 al 25 de 2008: **Australasian Information Security Conference AISC 2008 (Wollongong - Australia)** http://www.eng.newcastle.edu.au/~aisc2008/
Marzo 13 al 15 de 2008: **4th Workshop on Coding and Systems (Alicante y Elche - España)** http://www.dccia.ua.es/wcs2008
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/

CUALQUIER CONSULTA ENVIAR UN CORREO AL
CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION
CCISI
EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106