

Un informe revela fallos en el cortafuegos de Check Point.

Pentest Consultores acaba de publicar un exhaustivo informe sobre el cortafuegos de Check Point el buque insignia del gigante de la seguridad donde se ponen de manifiesto numerosos fallos de programación que cuestionan la integridad del ciclo de desarrollo del fabricante Israelí así como la validez de las certificaciones obtenidas. PenTest demuestra en su extenso informe de más de 200 páginas como aludir todos los mecanismos de seguridad del producto analizado.

El informe puede ser descargado de:

http://www.pentest.es/checkpoint_hack.pdf

No es el tipo de anuncio lo que supone una novedad, sino el objeto de análisis de dicho informe, la "Secure Platform", la versión de cortafuegos más segura de todas y que recientemente había sido certificada con el nivel EAL4+ de la Common Criteria.

La "Secure Platform" está basada una distribución Linux Red Hat Enterprise y un kernel -núcleo- parcheado con Exec-Shield, una protección desarrollada por Red Hat para detener la explotación de vulnerabilidades del tipo "buffer overflow". Dicha protección ofrece entre otros los siguientes mecanismos de seguridad:

- 1.- Las zonas de la memoria "Stack", "Heap", "BSS" y ".data" de un proceso no son ejecutables.
- 2.- ASLR (Address Space Layout Randomization).
- 3.- ASCII Armor (librerías mapeadas por debajo de 16 MB de memoria virtual).
- 4.- Direcciones base de la "stack" y de la "heap" aleatorias.

Las consecuencias directas de estas medidas de seguridad son:

- 1.- Los intrusos no pueden ejecutar código -shellcodes- de la manera tradicional, es decir "inyectandolo" en las zonas protegidas.
- 2.- Para cada carga de un binario las librerías tienen direcciones distintas, y por lo tanto los ataques tipo "Return-into-lib/libc" son. extremadamente complejos.
- 3.- Las direcciones en las que se mapean las librerías contienen un "null byte", dificultando en extremo la explotación de fallos debidos la manipulación de arrays de caracteres.

Como medida de protección adicional, la interfaz de gestión de la Secure Platform via línea de comandos es una shell especialmente adaptada por CheckPoint que solo permite el uso de un rango de caracteres ASCII muy restringido.

Todas estas medidas y el hecho de que el gobierno de los EEUU haya certificado esta plataforma [1]

han desatado la polémica en la prensa[2] internacional especializada de todo el mundo.

Para la solución de este tipo de problemas, PenTest Consultores recomienda el uso de sistemas con múltiples capas de seguridad, como por ejemplo los que permiten políticas MAC (Mandatory Access Control), sistemas MLS, etc. Por otro lado Pentest Consultores también recomienda la realización periódica de pruebas de intrusión independientes de los fabricantes, organismos oficiales y proveedores habituales a fin de obtener una "nueva perspectiva" de la seguridad.

Nota: Los analistas de Pentest Consultores llevan a cabo tests de intrusión para el sector de la banca, administraciones e industria desde 1998. La idiosincrasia de la compañía se basa en un modelo tipo "pull" [3] con "dedicación exclusiva por el cliente" según palabras de Luis Calero, nuevo director técnico de la empresa.

Referencias:

[1] Validation Report

http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID10091-VR.pdf

[2] Repercusión en medios:

<http://www.securityfocus.com/bid/25886/info>

http://www.theregister.co.uk/2007/10/03/check_point_pentest/

<http://www.heise.de/newsticker/meldung/96841>

<http://www.heise.de/security/news/meldung/96841/Mehrere-Buffer-Overflows-in-Checkpoints-Firewall-1-U>

<http://www.security.nl/article/17086/1/>

http://www.linux-magazine.com/online/news/holes_in_firewall_1

[3] "From Push to Pull-. Emerging Models for. Mobilizing Resources"

<http://www.johnseelybrown.com/pushmepullyou4.72.pdf>

Fecha artículo: 2007-10-10 18:49:38 - url artículo: <http://www.internautas.org/html/4325.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org