



Autor: Fernando Quintero (a.k.a nonroot)
Correo electrónico: fernando.a.quintero@gmail.com

Fecha de creación : 08/04/07

Ultima modificación: 08/04/07

Índice de contenido

1.Licencia (BSD).....	1
2.Introducción.....	2
3.Que es un parche (patch)?.....	2
4.Aplicando un parche real.....	3
5.Conclusiones.....	5

1. Licencia (BSD)

Copyright (c) 2007, Fernando Quintero,

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the **OpenBSD Colombia** nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

2. Introducción

Este mini documento explica de manera simple como se aplica un parche y para que se hace, el procedimiento es similar con cada parche en cada release de OpenBSD.

El aplicar parches es un proceso largo que muchas veces involucra reconstruir todo el sistema lo que en algunas maquinas puede tardarse varias horas, por eso mi recomendación es que si no tienes una maquina en producción y no estas tan paranoico solo busques los parches **ultra** importantes y descartes los otros.

3. Que es un parche (patch)?

Un parche es un trozo de código que se le inserta al código fuente de una aplicación o programa, esto con el fin de corregir errores o en definitiva, mejorarlo.

Pensemos en el siguiente ejemplo:

Existe un archivo llamado *linea* que contiene dos lineas de texto, pero una de las lineas tiene un error gramatical.

```
#cat linea
Esta linea tiene un erorr
Pero esta no
```

Supongamos que este es el código oficial, pero un día alguien descubre el error y quiere arreglarlo, entonces que haría?.

Puede tomar el archivo llamado *linea* y editarlo para corregir el error, de esta forma todo quedará solucionado en poco tiempo. Esto es cierto pero hay un pequeño inconveniente.

¿Como las personas que trabajan en el proyecto se darían cuenta que hubo un error y que alguien lo corrigió?

¿Como se llevaría un historial de los cambios que le sucedan a este archivo?

¿Como otra persona podría determinar si el cambio hecho por otro usuario es el correcto en vez de estar perjudicando el trabajo global de todos?

Como acabas de concluir tiene que haber otro mecanismo que me permita tener toda esta información y aún así realizar los cambios adecuados sobre el archivo.

La solución es que el usuario que quiera mejorar el archivo *linea*, haga una copia del mismo, luego arregle (parche) la copia y genere un parche que enviará al dueño original del archivo.

Si el dueño acepta aplicarle el parche este quedará registrado como *parche#1* y se le podrá hacer un seguimiento al archivo.

Supongamos entonces que el segundo usuario crea una copia y la edita:

```
#cp linea linea_buena
#nano linea_buena
Esta linea tiene un error
Pero esta no
```

Y luego genera un parche ...

```
#diff -u linea_buena linea > patch_linea
```

El parche se llama *patch_linea*, este nuevo archivo contiene las instrucciones de los cambios que se le aplicaran al archivo original en el caso de que el usuario propietario quiera aplicarlo.

Finalmente el dueño del archivo aplicaría el parche:

```
#patch -PO < patch_linea
```

En gráficas:

```
sh-2.05b#
sh-2.05b#
sh-2.05b#
sh-2.05b#
sh-2.05b# cat linea
Esta linea tiene un error
Pero esta no
sh-2.05b# cat linea_buena
Esta linea tiene un error
Pero esta no
sh-2.05b# diff -u linea_buena linea
--- linea_buena 2007-05-23 02:56:34.000000000 +0000
+++ linea       2007-05-23 02:56:46.000000000 +0000
@@ -1,2 +1,2 @@
-Esta linea tiene un error
+Esta linea tiene un error
 Pero esta no
sh-2.05b# diff -u linea linea_buena
--- linea       2007-05-23 02:56:46.000000000 +0000
+++ linea_buena 2007-05-23 02:56:34.000000000 +0000
@@ -1,2 +1,2 @@
-Esta linea tiene un error
+Esta linea tiene un error
 Pero esta no
sh-2.05b#
```

Fig 1. Observe que si se cambia el orden al usar diff, no se obtienen los mismos resultados

```
sh-2.05b# diff -u linea linea_buena > patch_linea
sh-2.05b# cat patch_linea
--- linea       2007-05-23 02:56:46.000000000 +0000
+++ linea_buena 2007-05-23 02:56:34.000000000 +0000
@@ -1,2 +1,2 @@
-Esta linea tiene un error
+Esta linea tiene un error
 Pero esta no
sh-2.05b# patch -p0 < patch_linea
```

Fig 2. El archivo *patch_linea* es el parche

El mas (+) y el menos (-) en el archivo parche, indica lo que se debe de remover y agregar al archivo original con el objetivo de arreglarlo. Con el comando de la ultima linea aplico el parche sobre el archivo original el cual queda arreglado.

4. Aplicando un parche real

Antes de aplicar un parche real debemos de tener el código fuente original en nuestro sistema, puesto que allí es donde se encuentran los errores. Los programas que usamos ya estan compilados y a menos que exista una técnica para parchar binarios en un futuro para OpenBSD no se podrá hacer nada con los binarios.

El procedimiento por ahora será, parchar las fuentes y reconstruir los binarios afectados.

Por ejemplo, busquemos el ultimo error importate que hubo en OpenBSD 4.0 y simulemos que queremos actualizar nuestro sistema. Hay varias opciones para hacer esto, pero por ahora solo pensaremos en descargar el parche y aplicarlo.

Lo primero que hay que hacer es visitar la página de “erratas”, este es el sitio donde se aloja la información sobre los parches de seguridad para el sistema.

<http://www.openbsd.org/errata.html>

y entramos por la release 4.0:

<http://www.openbsd.org/errata40.html>

La errata actual para la release 4.1 es <http://www.openbsd.org/errata41.html>

Podemos observar el anuncio **011**.

Note que solo son 11 anuncios importantes de seguridad, si bien solo se cuentan en la errata los bugs mas importantes o que afecten la seguridad del sistema directamente, es una cantidad baja comparada con cualquier otro sistema operativo :).

011: SECURITY FIX: April 4, 2007 *All architectures*
 Multiple vulnerabilities have been discovered in X.Org.
 XC-MISC extension ProcXCMiscGetXIDList memory corruption vulnerability, BDFont parsing integer overflow vulnerability, fonts.dir file parsing integer overflow vulnerability, multiple integer overflows in the XGetPixel() and XInitImage functions in ImUtil.c. [CVE-2007-1003](#), [CVE-2007-1351](#), [CVE-2007-1352](#), [CVE-2007-1667](#).
[A source code patch exists which remedies this problem.](#)

Hay esta una descripción del bug (error, fallo) y hay un enlace para bajarse el código fuente.

Lo siguiente es proceder a bajarnos el código del parche (**011_xorg.patch**).

Nuevamente, hay que recordar que para poder parchar nuestro sistema es necesario tener las fuentes de nuestro sistema operativo. Estas se encuentran en nuestro CD de instalación y NO se instalarán por defecto. También se pueden descargar del ftp oficial de OpenBSD¹.

Estoy hablando de los archivos *src.tar.gz* (código fuente del sistema en general) y *sys.tar.gz* (*código fuente del núcleo*), si no las tiene, las puede encontrar en el sitio oficial para su release.

[Para la versión 4.0 ---> ftp://ftp.openbsd.org/pub/OpenBSD/4.0/](ftp://ftp.openbsd.org/pub/OpenBSD/4.0/)

[Para la versión 4.1 ---> ftp://ftp.openbsd.org/pub/OpenBSD/4.1/](ftp://ftp.openbsd.org/pub/OpenBSD/4.1/)

Para desempaquetarla haremos algo como:

```
#tar -C /usr/src zfvx src.tar.gz
#tar -C /usr/src zfvx sys.tar.gz
```

Verifique que los directorios creados estén en: */usr/src* y */usr/src/sys*, *respectivamente*.

Luego de descargar el archivo del parche podemos leer en su encabezado:

¹ <ftp://ftp.openbsd.org/pub/OpenBSD/>

Apply by doing (aplicar haciendo):

```
cd /usr/XF4    # Assuming XF4 is in /usr/XF4
patch -p0 < O11_xorg.patch
```

And then rebuild and install (y entonces reconstruir e instalar):

```
make build
```

Cada parche me indica como aplicarlo y como reconstruir el sistema, **SI!**, cada vez que aplicamos un parche es necesario recompilar nuestro sistema :(

OpenBSD actualmente no tiene un sistema de actualización binaria como muchas otras distribuciones, esto no se ha hecho por muchas razones que no voy a exponer ahora.

Los comandos serian:

```
#cd /usr/XF4
#patch -p0 < /ruta/a/O11_xorg.patch
#make build
```

Observe que este es un parche para el entorno gráfico (X11) y en OpenBSD el entorno gráfico viene en unos paquetes o archivos aparte.

Si quiere aplicar el parche del ejemplo, deberá descargar el archivo *XF4.tar.gz* del sitio desde donde descargo los otros archivos fuentes y luego descomprimirlo en */usr*.

En algunos sistemas esto es mas fácil, pero créeme que esta es la forma mas segura.

Existen otras formas de aplicar parches, pero de eso hablaremos en otro momento.

5. Conclusiones

- Aplicar parches manualmente y desde el código fuente puede ser un proceso lento, pero es seguro, ya que nosotros mismos podemos verificar el parche, podemos verificar lo que agregaremos o quitaremos de nuestro sistema.
- En definitiva solo aplica los parches cuando realmente los necesites, puede haber un workaround funcional con el que puedas sobrevivir.
- Cuando existan varios parches en la página de erratas, debes aplicarlos en el orden en que aparecen. Siempre los parches vienen numerados como en el ejemplo: **011_xorg.patch**.
- Un parche mal aplicado puede corromper las fuentes del sistema, ten cuidado al aplicarlos.
- Los parches de la errata siempre se aplican contra la versión original de las fuentes, no con versiones mejoradas, snapshots, actualizaciones o versiones del CVS.
- Una forma de evitar parchar de uno en uno, es seguir la versión *current* de OpenBSD a través del CVS. De esta forma siempre estarás al día en aspectos de seguridad y nuevas características, sin embargo cualquier día tu sistema puede no ser tan estable (No se recomienda para entornos en producción).
- Usar OpenBSD sigue siendo divertido.