نوشته شده توسط root
سه شنبه ، 30 شهریور 1389 ، 10:36 - آخرین بروزرسانی سه شنبه ، 30 شهریور 1389 ، 11:24

دیروز یک نقص امنیتی جدید برای FreeBSD کشف شد که مربوط به برنامه bzip2 بود . همانطور که می دانیم ما از برنامه bzip2 برنامه بوسیله کردن فشرده . کنیم می استفاده فشرده فایل کردن خارج یا و فایل سازی فشرده برای bzip2 به بقیه برنامه ها مانند gzip دارای سرعت کمتری است و زمان بیشتری را باید صرف کرد هر چند که میزان فشرده سازی بوسیله برنامه bzip2 به مراتب بهتر از سایر برنامه ها می باشد .

اخیرا کشف شده که هنگامی فایلی را بوسیله این برنامه از حالت فشرده خارج می کنید معیار های لازم برای برای صحت یا درستی فایل باز شده بوسله سیستم درست چک نمی شود و چک نمی شود آیا فایل هایی که باز شده اند آیا با فایل اصلی تطابق دارد یا نه و آیا یکی است . این نقص خیلی بزرگی است و می تواند به attacker ها اجازه دهد در هنگام extract فایل های compress شده فایل های خود را بر روی سیستم طرف مقابل extract کنند و باعث بروز مشکل شوند .

برای رفع این نقص امنیتی می توانید از روش های زیر استفاده کنید و سیستم خود را ایمن کنید

۱- سیستم عامل FreeBSD خود را ممکن است نسخه های قدیمی تر مانند 6.4 یا 7 باشد به نسخه stable انها ارتقا دهید و به اصطلاح سیستم خود را stable کنید تا این مشکل رفع گردد.

۲- patch برای . کنید patch را خود عامل سیستم و کنید دانلود را اند شده ساخته نقص رفع برای که را هایی کردن باید مراحل زیر را طی کنید

دستور های زیر را برای دانلود patch های لازم در محیط متنی یا ترمینال اجرا کنید

```
fetch http://security.FreeBSD.org/patches/SA-10:08/bzip2.patch
fetch http://security.FreeBSD.org/patches/SA-10:08/bzip2.patch.asc
```

خوب با دستور بالا patch ها را در مسیر مشخصی دانلود می کنیم . حالا کافی است به شاخه زیر برویم

```
cd /usr/src
```

و دستور های زیر را اجرا کنیم

patch < /path/to/patch

با دستور بالا patch **ی را دانلود نمو ده ایم را به سورس سیستم** patch **می کنیم . در اینجا منظور از** patch to path **مسیر قرار گیری فایل های مربوط به** patch **است که قبلا دانلود کرده ایم .**

بعد از patch **حالا به شاخه زیر می رویم**

cd /usr/src/lib/libbz2

و دستور های زیر ار تایپ می کنیم و منتظر می مانیم که تمام دستور ها به خوبی اجرا شوند و به پایان برسند

make obj && make depend && make && make install

می بینیم که دستور های بالا ترکیبی از چند دستور هستند که با علامت && **از هم جدا شده اند که به تر تیب اول** make **سپس و** make **سپس و** make depend **سپس و** obj **.شد خواهند اجرا** make install

حالا کافی است سیستم را ریست کنیم و خیالمان راحت باشد که نقص امنیتی بزرگ رفع شده است .

۳- سومین روش که به روش patch binary **معروف است راحت ترین روش برای رفع این ضعف امنیتی می باشد . که البته باید سیستم شما حتما از کرنل** Generic **استفاده کنید . برای استفاده از روش** patch binary **کافی است در ترمینال دستور های زیر را اجرا کنیم .**

freebsd-update fetch
freebsd-update install

با دستور های بالا آخرین آپدیت ها و patch **ها برای سیستم عامل** FreeBSD **دانلود و نصب خواهد شد . حالا کافی است سیستم خود را ریست کنیم و دستور زیررا پس ریست سیستم در ترمینال اجرا کنیم**

uname -a

خروجی باید چیزی شبیه به زیر باشد

نوشته شده توسط root
سه شنبه ، 30 شهریور 1389 ، 10:36 - آخرین بروزرسانی سه شنبه ، 30 شهریور 1389 ، 11:24

FreeBSD mfaridipc.faridi 8.1-RELEASE FreeBSD 8.1-RELEASE-p1 #0

حرف p1 **نشان می دهد که سیستم شما یکبار** patch **شده است . در حالی که قبل از این شما عبارت** p1 **را در خروجی** uname -a **.نداشتید**