TenFourFox Development

What's new in TenFourFox, the Mozilla browser for Power Macs.

Thursday, September 25, 2014

Bashing bash one more time: updated universal 4.3.26 covering both bash flaws

See the previous entry, but in short, `bash` has been shown to have a pretty nasty little vulnerability that causes it to inadvertently execute shell commands in the environment you pass it. This attack does work on Power Macs because most shell commands are cross-platform, and appears to exist on all versions of OS X.

The solution is easy: build a new `bash` from the newly patched source code. As a service to you, I have done so, and compiled it for PowerPC and Intel so it will also work for users on 10.6 who are not receiving updates either. **The version earlier today had a preliminary version of the patch which does not fix a second variant vulnerability. This version does. If you used one of the "build from source" tricks that were circulating earlier today (MacRumors, etc.), your version does NOT have this second issue patched. Either wait for the public source trees to update and rebuild it (likely early tomorrow), or use this one.**

The `bash` these steps will install works on 10.4 all the way to 10.9 on 32-bit Intel, 64-bit Intel and PowerPC. It requires no other dependencies. The idea is to replace your system `bash` -- yes, you can use Homebrew, Tigerbrew, MacPorts, etc., to get an updated copy, but your built-in `bash` is still vulnerable unless you replace it. This is designed to accomplish that. **WARNING AGAIN:** If you are not comfortable with the `Terminal`, get someone to help you!

1. In a `Terminal.app` window, verify that you have a vulnerable system so that you can see what that looks like (the command is all one line):

   ```
   env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
   ```

   It should print

   ```
   vulnerable
   this is a test
   ```

2. Check the second vulnerability. This creates a file called `echo` with the date in it, if your system is vulnerable:

   ```
   env X='() { (a)=>\' sh -c "echo date"; cat echo
   ```

   It should print something like (the messages and of course the time will vary):

   ```
   bash: X: line 1: syntax error near unexpected token `='
   bash: X: line 1: `'
   bash: error importing function definition for `X'
   Thu Sep 25 22:12:49 PDT 2014
   ```

Download TenFourFox

- TenFourFox Main Page
- TenFourFox User Support
- Project Site
- Wiki and FAQ
- File Repository

Fellow Fighters of the POWER

- PPC Luddite
- iFixOldMacs
- System Folder
- viva PowerPC
- MistyDeMeo.com
- TigerOSX
- LowEndMac

Blog Archive

September (8)
August (5)
July (8)
June (5)
May (6)
April (9)
March (6)
February (3)
January (3)
December (6)
November (8)
October (6)
September (6)
August (10)
July (6)
June (6)
May (8)
April (9)
March (8)
February (7)
January (3)
December (5)
November (8)
October (9)

(Delete the file it makes before you continue! `rm echo`)

3. Download the patched `bash` 4.3.26. Put it in your home directory. If necessary, double-click to decompress it so that you have a file in your home directory called `bash-4.3.26-10.4u`.

4. Close all terminal windows and programs just to make sure you won't stomp on `bash` while a program is trying to call it. Start `Terminal` and have exactly *one* window open.

5. In that terminal window:

    - `exec tcsh`
    - `chmod +x bash-4.3.26-10.4u`

    If you replaced `/bin/bash` (and/or `/bin/sh`) with the patch earlier today, **DO NOT DO THE NEXT TWO COMMANDS.** If you have *not* already replaced them, go ahead; these will put the old ones in a safe place, just in case.

    - `sudo mv /bin/bash /bin/bash_old` (enter your password)
    - `sudo mv /bin/sh /bin/sh_old` (enter your password if needed)

    Everybody does these:

    - `sudo cp bash-4.3.26-10.4u /bin/bash` (enter your password if needed)
    - `sudo cp bash-4.3.26-10.4u /bin/sh` (enter your password if needed)

6. Test it stuck by trying the statements again:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

It should print

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
this is a test
```

Now, try the second one:

```
env X='() { (a)=>\' sh -c "echo date"; cat echo
```

It should print

```
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
date
cat: echo: No such file or directory
```

7. Restart your Mac as a paranoia to make sure everything is using the new copy of `bash`.

8. Bask in the glow. Then, find a shell that doesn't suck.

Posted by ClassicHasClass at 10:21 PM

+1 Recommend this on Google

September (2)
August (4)
July (4)
June (4)
May (3)
April (5)
March (6)
February (6)
January (6)
December (9)
November (5)
October (3)
September (3)
August (6)
July (5)
June (5)
May (6)
April (6)
March (5)
February (5)
January (5)
December (5)
November (2)

Labels

- security (36)
- mozilla (16)
- qte (10)
- anfscd (9)
- PowerPC (7)
- ppc970 (6)
- applesnark (5)
- shame (5)
- transition (5)
- judgment day (4)
- mte (4)
- shoutout (2)
- 68k (1)
- classilla (1)
- intel (1)
- kubrick (1)
- sluggo (1)
- statistics (1)

About Me

ClassicHasClass

I like old Macs. And I like music. And I like Girls. And that's it. -- apologies to Sparks

View my complete profile

5 comments:

mwschmeer September 26, 2014 at 11:31 AM

Thank you! This is exactly what I was looking for to protect my old but treasured PPC Macs.

Reply

eb2d158c-45ab-11e4-818c-5317d593f061 September 26, 2014 at 11:37 AM

Thanks for posting this ClassicHasClass. I have two Tiger servers where I've tried to follow patch methods outlined elsewhere and each crashes upon executing the xcodebuild command. I hope to try your method soon once I build up the confidence to hit the command line again. :-)

Reply

joffreyca September 26, 2014 at 12:03 PM

Thanks for posting this. Patched applied to a Mac OS X 10.5.8 Server on a PowerMac G5.

Reply

verdant September 26, 2014 at 5:12 PM

verdant

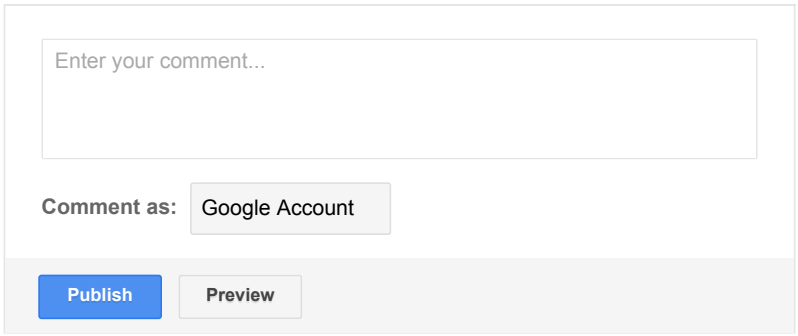
Fantastic - thanks so much for your public spirit in providing this universal patch for PPC/Intel and 10.4 thru to 10.9 so quickly! I have both PPC and Intel OS X 10.4 thru to 10.9 systems that are now protectable agains both bash vulnerabilities.

Reply

Simon Beazley September 26, 2014 at 11:15 PM

I couldn't get this to work on my G4 MDD running Mac OSX 10.5.8...

Reply



Due to an increased frequency of spam, comments are now subject to moderation.

Subscribe to: Post Comments (Atom)

Copyright 2014 Cameron Kaiser. All rights reserved. You are free to copy and use as you see fit. Simple template. Powered by Blogger.