

Forum:[Hack Forums](#)

Thread: [New root exploit for Yosemite: Rootpipe](#)

PeregrineX - April 25, 2015, 6:02 pm

I'm surprised nobody's started a discussion on this.

Exploit-DB: Google it. Can't post links yet.

For all you Mac nerds: there is a new local root exploit, codenamed "rootpipe." It is for Yosemite, although the author states it should work for earlier versions. It exploits the system by abusing a hidden admin API framework call.

It already has a CVE: 2015-1130. Apple has tried to patch this in Yosemite recently, however, it flopped.

So, don't download ANY suspicious apps, especially new ones, until they really patch this. If you intend to use this exploit for your own nefarious purposes, go ahead.

Any thoughts? Will you be using this? Discuss below. ???

w34k - April 28, 2015, 10:06 pm

I believe it was patched with the latest update of OS X 10.10.3

<https://support.apple.com/en-us/HT204659>

PoC of the exploit here.

<https://truesecdev.wordpress.com/2015/04/09/hidden-backdoor-api-to-root-privileges-in-apple-os-x>

I think it's funny how it's been around for that long. Makes you wonder what else is just waiting to be found.

Statesman - April 29, 2015, 3:54 am

(Apr 25, 2015 06:02 PM)PeregrineX Wrote: [\[CITE\]](#) I'm surprised nobody's started a discussion on this.

Exploit-DB: Google it. Can't post links yet.

For all you Mac nerds: there is a new local root exploit, codenamed "rootpipe." It is for Yosemite, although the author states it should work for earlier versions. It exploits the system by abusing a hidden admin API framework call.

It already has a CVE: 2015-1130. Apple has tried to patch this in Yosemite recently, however, it flopped.

So, don't download ANY suspicious apps, especially new ones, until they really patch this. If you intend to use this exploit for your own nefarious purposes, go ahead.

Any thoughts? Will you be using this? Discuss below. ???

You don't know this was patched successfully last update ?? ?

