

Forum:[Hack Forums](#)

Thread: [\[Need\] 2.6.18-194.32.1 2011 i686 local root exploit](#)

Jack_ - August 7, 2013, 11:51 am

As the title says I want/need a local root exploit for this version

Code 2.6.18-194.32.1 2011 i686

I have searched for it but I have not found it.

Krieg - August 7, 2013, 1:35 pm

<http://grsecurity.net/~spender/exploits/enlightenment.tgz>

I fucking swear if you come back and tell me there's no compiler on the box I'll stab you in the face 666 times.

SoLong - August 7, 2013, 2:18 pm

(Aug 7, 2013 01:35 PM)Krieg Wrote: [\[CITE\]](#) <http://grsecurity.net/~spender/exploits/enlightenment.tgz>

I fucking swear if you come back and tell me there's no compiler on the box I'll stab you in the face 666 times.

There is no compiler on the box :((

webcreator - August 7, 2013, 4:45 pm

mmh, maybe i have the solution for u,
contact me in pm

n3xus - August 7, 2013, 5:07 pm

(Aug 7, 2013 02:18 PM)SoLong Wrote: [\[CITE\]](#) There is no compiler on the box :((
compile them on your own box/vm, then upload them to the box you are trying to own.

SoLong - August 7, 2013, 5:31 pm

(Aug 7, 2013 05:07 PM)n3xus Wrote: [\[CITE\]](#) compile them on your own box/vm, then upload them to the box you are trying to own.

It was a reply to Krieg's post :D
dirtyfive

pashabiceps - August 8, 2013, 6:19 am

(Aug 7, 2013 05:07 PM)n3xus Wrote: [\[CITE\]](#) compile them on your own box/vm, then upload them to the box you are trying to own.

Isn't that rather obvious?

Oh sorry, this is HF.

Jack_ - August 9, 2013, 9:55 am

(Aug 7, 2013 01:35 PM)Krieg Wrote: [\[CITE\]](#) <http://grsecurity.net/~spender/exploits/enlightenment.tgz>

I fucking swear if you come back and tell me there's no compiler on the box I'll stab you in the face 666 times.

I downloaded it and compiled it. When I tried executing the file pwnkernel. I get an error that it cannot execute it the same with the other binaries. Are you sure that is the right exploit? Some of the files on the folder are outdated.

Krieg - August 9, 2013, 10:13 am

Paste the error, please.

If it's "Cannot execute binary file" then you've failed and you need to think about what you've done wrong.

Spoiler ([Click to View](#))

Wrong CPU architecture.

Jack_ - August 9, 2013, 10:44 am

(Aug 9, 2013 10:13 AM)Krieg Wrote: ([CITE](#)) Paste the error, please.

If it's "Cannot execute binary file" then you've failed and you need to think about what you've done wrong.

Spoiler ([Click to View](#))

Wrong CPU architecture.

That is the error I'm getting. So the exploit is for 64 bit?

Krieg - August 9, 2013, 5:07 pm

No. You compiled it on (or for) a 64bit box and are trying to run it on 32bit. This won't work.

Jack_ - August 12, 2013, 9:52 am

I compiled them on a 32 computer and when I try to run the file exploit I get

Code ./exploit: /lib/libc.so.6: version 'GLIBC_2.7' not found (required by ./exploit)

The pwnkernel didn't work I get

Code Pulseaudio does not exist!

Does anyone have an idea on how to proceed?

Krieg - August 12, 2013, 9:53 am

You should be running the NON null exploits, anyway...

Jack_ - August 12, 2013, 9:58 am

(Aug 12, 2013 09:53 AM)Krieg Wrote: ([CITE](#)) You should be running the NON null exploits, anyway...

That is what I'm doing and I get the following error

Code ./exploit: /lib/libc.so.6: version 'GLIBC_2.7' not found (required by ./exploit)

The second error is for the null exploits.

Krieg - August 12, 2013, 10:03 am

Code ./exploit: /lib/libc.so.6: version 'GLIBC_2.7' not found (required by ./exploit) This is saying that you compiled for a newer version of Glibc than is available on the target system.

You need to link the executable to older glibc functions, or compile it with the -static flag.

Jack_ - August 12, 2013, 10:33 am

(Aug 12, 2013 10:03 AM)Krieg Wrote: ([CITE](#)) Code ./exploit: /lib/libc.so.6: version 'GLIBC_2.7' not found (required by ./exploit) This is saying that you compiled for a newer version of Glibc than is available on the target system.

You need to link the executable to older glibc functions, or compile it with the -static flag.

So how would I do that using the run_nonnull_exploits.sh file? Or just use

Code gcc exploit.c -static -o exploit

Krieg - August 12, 2013, 10:36 am

Look at the script and see how it's compiling ./exploit, copy the line it uses and just add the -static flag to gcc.

??s?? - August 12, 2013, 11:16 am

[Video: http://www.youtube.com/watch?v=sCDN0r4_L58]

Krieg - August 12, 2013, 11:19 am

(Aug 12, 2013 11:16 AM)??s?? Wrote: [\[CITE\]](#) -snip tard vid-

You could actually teach how to adapt instead of embedding videos, but you're too high quality for that.

The exploit used in the video isn't even shown. It's just some mysterious Perl script that the guy doesn't even provide.

Sure does help a fuck lot when you post videos of an exploit that's not even provided. Some "teacher" you are, big guy.

??s?? - August 12, 2013, 11:28 am

(Aug 12, 2013 11:19 AM)Krieg Wrote: [\[CITE\]](#) You could actually teach how to adapt instead of embedding videos, but you're too high quality for that.

The exploit used in the video isn't even shown. It's just some mysterious Perl script that the guy doesn't even provide.

Sure does help a fuck lot when you post videos of an exploit that's not even provided. Some "teacher" you are, big guy.

I'm on a mobile device, excuse me if I'm not here to type out an entire monologue.

Turn down the flames, kid.

Krieg - August 12, 2013, 11:29 am

(Aug 12, 2013 11:28 AM)??s?? Wrote: [\[CITE\]](#) I'm on a mobile device, excuse me if I'm not here to type out an entire monologue.

Turn down the flames, kid.

How 'bout you turn up the intelligence first and actually help? Posting videos in which the process isn't even shown doesn't do anything.

Nyckel - August 12, 2013, 11:30 am

(Aug 12, 2013 11:28 AM)??s?? Wrote: [\[CITE\]](#) Turn down the flames, kid.

OO HE USED THE K WORD!!1!!!!11!!11two!!

SHIT'S ABOUT TO GO DOWN.

Krieg - August 12, 2013, 11:31 am

This is beyond hilarious. OP, if you'd like some more assistance you can PM me with the shell and I'll just pop it for you.

Offtopic: someone's upset that a non-upgraded is better than him.

brown8813 - October 13, 2013, 2:31 pm

Jack, your inbox so I cant send you messages - contact me as soon as you can.

Trojan Man™ - July 24, 2014, 11:09 am

sent you payment for the downloader.

will open a scam report if you do not send me source.

Trojan Man™ - July 25, 2014, 11:29 pm

beware user is a scammer.

<https://hackforums.net/showthread.php?tid=4359966>