

Re: Linux hardening

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2005-08/0066.html>

From: Jon Hart (warchild_at_spoofed.org)

Date: 08/24/05

Date: Wed, 24 Aug 2005 17:39:48 -0400
To: Craig Holmes <leusent@link-net.org>

On Wed, Aug 24, 2005 at 01:11:58AM -0400, Craig Holmes wrote:

> *On Sunday 21 August 2005 08:13, AragonX wrote:*
> > *I'm looking for more preventative measures. It appears that LIDS and*
> > *mod_security are the only ones in that role now.*
> *I recommend tuning php and disabling commands like system and passthru that*
> *may be used by an attacker but are probably not going to be used by you. I*
> *like to think that no webpage or script can be trusted even when I am the*
> *only person with access to a machine.*
>
> *Many people have recommended mounting /tmp and /var/tmp noexec. This is a good*
> *idea but keep in mind that it is easy to execute commands even on a noexec*
> *filesystem (using the ld-linux library). So don't be surprised if some*
> *slightly clever attacker is running a binary from that location.*

Is this still possible? I thought this was fixed with newer kernel versions. If this does indeed fix the problem of using ld-linux to bypass noexec permissions, are there other ways around it?

```
$ mount
$ cd /tmp
$ mount |grep tmp
tmpfs on /dev/shm type tmpfs (rw,noexec,nosuid,nodev)
/dev/hda5 on /tmp type ext3 (rw,noexec,nosuid,nodev)
$ cat test.c
int main() {
    printf("Test\n");
    exit(0);
}
$ gcc -o test test.c
$ ./test
bash: ./test: Permission denied
$ /lib/ld-linux.so.2 ./test
./test: error while loading shared libraries: ./test: failed to
map segment from shared object: Operation not permitted
```

-jon