Subject: Kernel Root Exploit?
Posted by mperkel on Mon, 11 Feb 2008 18:08:52 GMT
View Forum Message <> Reply to Message

Someone alerted me to this.

https://bugzilla.redhat.com/show_bug.cgi?id=432229

Description of problem:

Local user can obtain root access (as described below).

This bug is being actively exploited in the wild -- our server was just broken
in to by an attacker using it. (They got a user's password by previously
compromising a machine somewhere else where that user had an account, and
installed a modified ssh binary on it to record user names and passwords. Then
they logged in to our site as that user, exploited CVE-2008-0010, and became root).

It is EXTREMELY urgent that a fixed kernel be provided ASAP given that this bug
is being actively exploited in the wild.

There is a fix listed upstream in 2.6.23.15 and 2.6.24.1. However, even after
applying that patch and recompiling the kernel, the escalation-of-privilege
exploit still worked so I am wondering if 2.6.23.15 does not completely fix it.

Version-Release number of selected component (if applicable):

All 2.6.23.x kernels

How reproducible: 100%

Steps to Reproduce:
1. Download http://downloads.securityfocus.com/vulnerabilities/exploits/ 27704.c
2. cc -o exploit 27704.c
3. [as non-privileged user] ./exploit

Actual results:

Root shell

Expected results:

No root shell.

Additional info:

When I altered the kernel spec file for 2.6.23.14-115.fc8 to pull 2.6.23.15
instead of 2.6.23.14 (and altered linux-2.6-highres-timers.patch to apply

cleanly, and removed the already-included-in-2.6.23.15 patches linux-2.6-net-silence-noisy-printks.patch and linux-2.6-freezer-fix-apm-emulation-breakage.patch), rebuilt a new kernel RPM, installed it, and rebooted, the above exploit still worked. So it is possible an additional patch is needed against 2.6.23, unless I just goofed somehow in my kernel rebuild. (I did check and the file fs/splice.c was correctly patched and included the lines that were suppose to fix this problem...)

More info:

Marc,

Even better:

http://home.powertech.no/oystein/ptpatch2008/
