Subject: 2.6.22/2.6.18 security fixes
Posted by Josip Rodin on Wed, 13 Feb 2008 00:10:27 GMT
View Forum Message <> Reply to Message

Hi,

It would be useful if the linux-2.6.22-openvz tree included the security
fixes added in the later versions of the 2.6.22 kernel. Notably:

http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.22.y.git;a=commitdiff;h=af395d8632d0524be27d8774a1607e68bdb4dd7f
http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.22.y.git;a=commitdiff;h=53d06121542c36ec0f0e5504c8358a768e25cb9a

Does the 'frozen' tag preclude including these things? The 2.6.22 kernel is
still described as maintained on the main web site, so it would make sense
to add those fixes.

At the same time, the linux-2.6.18-openvz tree is missing the fs/splice.c
fix for get_iovec_page_array(), WRT the latest local root exploit. There
is no upstream git reference for that, because stable/linux-2.6.18.y.git
appears to be long abandoned, so here's the patch:

```
--- linux-2.6.18/fs/splice.c~ 2008-02-12 00:34:49.000000000 +0100
+++ linux-2.6.18/fs/splice.c 2008-02-12 00:34:49.000000000 +0100
@@ -1122,6 +1122,11 @@
  size_t len;
  int i;

+  if (!access_ok(VERIFY_READ, iov, sizeof(struct iovec))) {
+   error = -EFAULT;
+   break;
+  }
+
  /*
   * Get user address base and length for this iovec.
   */
@@ -1141,6 +1146,11 @@
  if (unlikely(!base))
   break;

+  if (!access_ok(VERIFY_READ, base, len)) {
+   error = -EFAULT;
+   break;
+  }
+
  /*
   * Get this base offset and number of pages, then map
```

* in the user pages.

--
2. That which causes joy or happiness.

Subject: Re: 2.6.22/2.6.18 security fixes
Posted by kir on Mon, 18 Feb 2008 15:28:46 GMT
View Forum Message <> Reply to Message

The fix for this issue was included into 2.6.18 kernels .spec file (to release the fix faster). Now we pushed that to git, too, it is available.

2.6.24 kernel (not yet released) was just synced to latest 2.6.24.2 update, which covers the security issue as well.

2.6.20 and 2.6.22 are frozen, means they are obsoleted and unmaintained.

Regards,
Kir.

Josip Rodin wrote:
> Hi,
>
> It would be useful if the linux-2.6.22-openvz tree included the security
> fixes added in the later versions of the 2.6.22 kernel. Notably:
>
>
http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.22.y.git;a=commitdiff;h=af395d8632d0524be27d8774a1607e68bdb4dd7f
>
http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.22.y.git;a=commitdiff;h=53d06121542c36ec0f0e5504c8358a768e25cb9a
>
> Does the 'frozen' tag preclude including these things? The 2.6.22 kernel is
> still described as maintained on the main web site, so it would make sense
> to add those fixes.
>
> At the same time, the linux-2.6.18-openvz tree is missing the fs/splice.c
> fix for get_iovec_page_array(), WRT the latest local root exploit. There
> is no upstream git reference for that, because stable/linux-2.6.18.y.git
> appears to be long abandoned, so here's the patch:
>
> --- linux-2.6.18/fs/splice.c~ 2008-02-12 00:34:49.000000000 +0100
> +++ linux-2.6.18/fs/splice.c 2008-02-12 00:34:49.000000000 +0100
> @@ -1122,6 +1122,11 @@

```
>    size_t len;
>    int i;
>
> +  if (!access_ok(VERIFY_READ, iov, sizeof(struct iovec))) {
> +    error = -EFAULT;
> +    break;
> +  }
> +
>    /*
>     * Get user address base and length for this iovec.
>     */
> @@ -1141,6 +1146,11 @@
>    if (unlikely(!base))
>     break;
>
> +  if (!access_ok(VERIFY_READ, base, len)) {
> +    error = -EFAULT;
> +    break;
> +  }
> +
>    /*
>     * Get this base offset and number of pages, then map
>     * in the user pages.
>
>
```