Subject: Problem with patch by openvz, where should I report that?
Posted by ml-openvz-eyck on Sat, 15 Sep 2007 09:11:27 GMT
View Forum Message <> Reply to Message

The patch is: core-dumping unreadable binaries via PT_INTERP
it's described as:

"
From: Alexey Dobriyan <adobriyan@openvz.org>
Date: Fri, 26 Jan 2007 08:57:16 +0000 (-0800)
Subject: [PATCH] core-dumping unreadable binaries via PT_INTERP
X-Git-Tag: v2.6.20-rc7^0~60
X-Git-Url:
http://git.kernel.org/?p=linux%2Fkernel%2Fgit%2Ftorvalds%2Flinux-2.6.git;a=commitdiff_plain;h=1fb844961818ce94e782acf6a96b92dc2303553b

[PATCH] core-dumping unreadable binaries via PT_INTERP

Proposed patch to fix #5 in
http://www.isec.pl/vulnerabilities/isec-0017-binfmt_elf.txt

....
Check for MAY_READ like binfmt_misc.c does.

Signed-off-by: Alexey Dobriyan <adobriyan@openvz.org>
Signed-off-by: Andrew Morton <akpm@osdl.org>
Signed-off-by: Linus Torvalds <torvalds@linux-foundation.org>
"

and when applied to 2.6.18 ovz028stab039.1, it stops my kernels
from booting ( they fail to find root filesystem in initrd and
hang there waiting for it to appear ).
 Where do I report it ( or maybe how can I check if this has been
fixed in the meantime? )

--
Key fingerprint = 40D0 9FFB 9939 7320 8294  05E0 BCC7 02C4 75CC 50D9
 Total Existance Failure

Subject: Re:  Problem with patch by openvz, where should I report that?
Posted by dev on Mon, 17 Sep 2007 07:01:59 GMT
View Forum Message <> Reply to Message

This patch just disables core file from some of the executables.
Not sure how it can affect your initrd... Only if it crashes somewhere,
which should not normally happen.
Can you please recheck, that this is exactly this patch?

Plus, I don't understand how you managed to apply this patch to 028stab039.
This patch is already included in OpenVZ kernels since long ago 028test015...
So maybe it was applied by you 2nd time somehow and with wrong context?

Thanks,
Kirill

Dariush Pietrzak wrote:
> The patch is: core-dumping unreadable binaries via PT_INTERP
> it's described as:
>
> "
> From: Alexey Dobriyan <adobriyan@openvz.org>
> Date: Fri, 26 Jan 2007 08:57:16 +0000 (-0800)
> Subject: [PATCH] core-dumping unreadable binaries via PT_INTERP
> X-Git-Tag: v2.6.20-rc7^0~60
> X-Git-Url:
>
http://git.kernel.org/?p=linux%2Fkernel%2Fgit%2Ftorvalds%2Flinux-2.6.git;a=commitdiff_plain;h=
1fb844961818ce94e782acf6a96b92dc2303553b
>
> [PATCH] core-dumping unreadable binaries via PT_INTERP
>
> Proposed patch to fix #5 in
> http://www.isec.pl/vulnerabilities/isec-0017-binfmt_elf.txt
>
> ....
> Check for MAY_READ like binfmt_misc.c does.
>
> Signed-off-by: Alexey Dobriyan <adobriyan@openvz.org>
> Signed-off-by: Andrew Morton <akpm@osdl.org>
> Signed-off-by: Linus Torvalds <torvalds@linux-foundation.org>
> "
>
> and when applied to 2.6.18 ovz028stab039.1, it stops my kernels
> from booting ( they fail to find root filesystem in initrd and
> hang there waiting for it to appear ).
>  Where do I report it ( or maybe how can I check if this has been
> fixed in the meantime? )
>

---

Subject: Re:  Problem with patch by openvz, where should I report that?
Posted by ml-openvz-eyck on Mon, 17 Sep 2007 07:36:22 GMT
View Forum Message <> Reply to Message

On Mon, 17 Sep 2007, Kirill Korotaev wrote:

> Plus, I don't understand how you managed to apply this patch to 028stab039.
> This patch is already included in OpenVZ kernels since long ago 028test015...
> So maybe it was applied by you 2nd time somehow and with wrong context?
 My bad, it got applied 2nd time, resulting in garbled, but compilable
code, but it applies rather cleanly to 028stab039, and patch does not
complain that the patch is reversed, which is rather unusual.
 I guess the fact that patch just adds lines and not modifies anything
helped.

 How should I go about applying bugfixes to 028stab039, I went through list
of bugfixes for 2.6.18 and applied them to ovz sources when one of my
machines got oops that is fixable by this:

X-Git-Url:
http://git.kernel.org/?p=linux%2Fkernel%2Fgit%2Ftorvalds%2Flinux-2.6.git;a=commitdiff_plain;h=
9ad0830f307bcd8dc285cfae58998d43b21727f4
[PATCH] Keys: Fix key serial number collision handling

 since ovz contains some of the fixes, and omits some others, I had
to check this experimentally - I skipped those that are already applied
(which I test by check if reversed patch applies) and applied only those
that could be applied with little fuzz... the PT_INTERP patch
unfortunatelly went through the procedure as 'not already applied and
applying cleanly'.

 Maybe some list of fixes allready included in given ovz patch would help
in avoiding similar situation in the future, would it be possible to get
such list?

regards, eyck
--
Key fingerprint = 40D0 9FFB 9939 7320 8294  05E0 BCC7 02C4 75CC 50D9
 Total Existance Failure

---

Subject: Re:  Problem with patch by openvz, where should I report that?
Posted by dev on Fri, 21 Sep 2007 14:26:54 GMT
View Forum Message <> Reply to Message

>  since ovz contains some of the fixes, and omits some others, I had
> to check this experimentally - I skipped those that are already applied
> (which I test by check if reversed patch applies) and applied only those
> that could be applied with little fuzz... the PT_INTERP patch
> unfortunatelly went through the procedure as 'not already applied and
> applying cleanly'.
>

> Maybe some list of fixes allready included in given ovz patch would help
> in avoiding similar situation in the future, would it be possible to get
> such list?

git.openvz.org has all the patches, but it's not easy to look through
this list as it is quite big.
We try to add all the patches which fall in the following categories:
- security
- bugs faced by OVZ users
- bugs we found and fixed ourself.

The patch is question was found & fixed by Alexey Dobriyan - one of our developers,
so the fix is here.

Thanks,
Kirill

---