Universidad Zaragoza

CVE-2022-27666: exploit esp6 modules in Linux kernel

Guillermo Cruz Rojas

10/01/2024

CVE-2022-27666

-

Exploit esp6 modules in Linux Kernel

Guillermo Cruz Rojas
682433@unizar.es

Exploiting Software Vulnerabilities

Master's Degree in Informatics Engineering

Vulnerability Characterization

What are esp6 modules?

- esp6 -> **E**ncapsulating **S**ecurity **P**ayload IPv**6**

Vulnerability Characterization

What are esp6 modules?

- esp6 -> **E**ncapsulating **S**ecurity **P**ayload IPv**6**

Encapsulating Security Payload (ESP) [1]

- Is one of the protocols that implement the open standard **IPsec** (Internet Protocol Security)

[1] https://en.wikipedia.org/wiki/IPsec

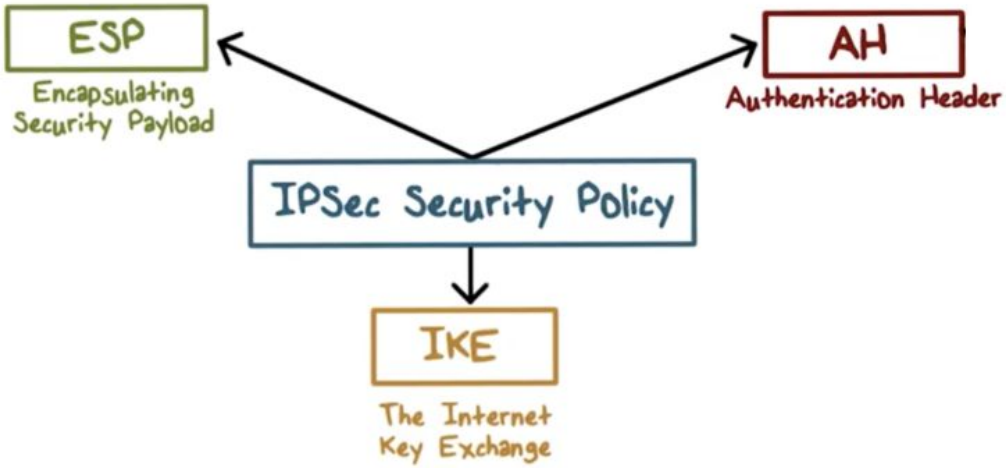
Vulnerability Characterization

What are esp6 modules?

- esp6 -> **E**ncapsulating **S**ecurity **P**ayload IPv**6**

Encapsulating Security Payload (ESP) [1]

- Is one of the protocols that implement the open standard **IPsec** (Internet Protocol Security)
- IPsec is a secure network protocol suite that authenticates and encrypts packets of data between two computers over an Internet Protocol network (layer 3)



[1] https://en.wikipedia.org/wiki/IPsec

Vulnerability Characterization

CVE-2022-27666 Detail (nvd.nist.gov) [1]

- **Description**
  - A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat.

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-27666

Vulnerability Characterization

CVE-2022-27666 Detail (nvd.nist.gov) [1]

- **Description**
  - A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat.

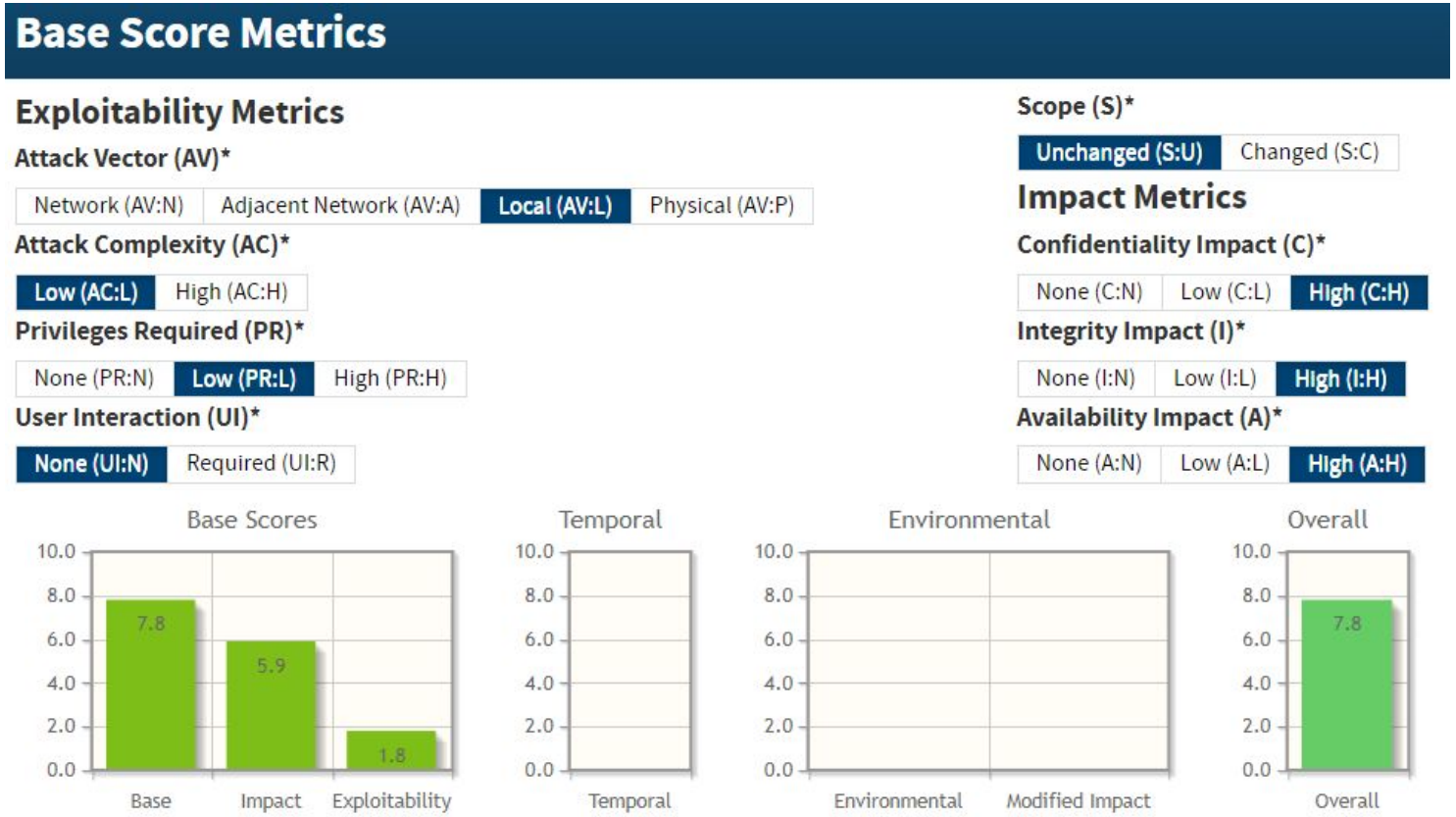
- **Severity**

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-27666

Vulnerability Characterization

CVE-2022-27666 Detail (nvd.nist.gov) [1]

- **Severity**



[1] https://nvd.nist.gov/vuln/detail/CVE-2022-27666

Technical Description

Vulnerability Root Cause

- Introduced in Linux Kernel by commit 03e2a30f6a27 (esp6) and commit cac2661c53f3 (esp4) in 2017 [1]

[1] https://etenal.me/archives/1825

Technical Description

Vulnerability Root Cause

- Introduced in Linux Kernel by commit 03e2a30f6a27 (esp6) and commit cac2661c53f3 (esp4) in 2017 [1]

- The receiving buffer of a user message in esp6 module is an 8-page buffer, but the sender can send a message larger than 8 pages, creating a buffer overflow

[1] https://etenal.me/archives/1825

Technical Description

Vulnerability Root Cause

- Introduced in Linux Kernel by commit 03e2a30f6a27 (esp6) and commit cac2661c53f3 (esp4) in 2017

net/ipv6/esp6.c

```
@@ -200,19 +252,130 @@ static int esp6_output(struct xfrm_state *x, struct sk_buff *skb)
                assoclen += seqhilen;
        }

                                ...

+
+                       int allocsize;
+                       struct sock *sk = skb->sk;
+                       struct page_frag *pfrag = &x->xfrag;
+
+                       allocsize = ALIGN(tailen, L1_CACHE_BYTES);
+
+                       spin_lock_bh(&x->lock);
+
+                       if (unlikely(!skb_page_frag_refill(allocsize, pfrag, GFP_ATOMIC))) {
+                               spin_unlock_bh(&x->lock);
+                               goto cow;
+                       }
+
+                       page = pfrag->page;
+                       get_page(page);
                                ...
```

Source: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=03e2a30f6a27e2f3e5283b777f6ddd146b38c738

Technical Description

Vulnerability Root Cause

- Introduced in Linux Kernel by commit 03e2a30f6a27 (esp6) and commit cac2661c53f3 (esp4) in 2017

net/core/sock.c

```
bool skb_page_frag_refill(unsigned int sz, struct page_frag *pfrag, gfp_t gfp)

        ...

    pfrag->offset = 0;
    if (SKB_FRAG_PAGE_ORDER) {
        /* Avoid direct reclaim but allow kswapd to wake */
        pfrag->page = alloc_pages((gfp & ~__GFP_DIRECT_RECLAIM) |
                                  __GFP_COMP | __GFP_NOWARN |
                                  __GFP_NORETRY,
                                  SKB_FRAG_PAGE_ORDER);
        if (likely(pfrag->page)) {
            pfrag->size = PAGE_SIZE << SKB_FRAG_PAGE_ORDER;
            return true;
        }
    }

        ...
```

Technical Description

Vulnerability Root Cause

- Introduced in Linux Kernel by commit 03e2a30f6a27 (esp6) and commit cac2661c53f3 (esp4) in 2017

net/core/sock.c

```
bool skb_page_frag_refill(unsigned int sz, struct page_frag *pfrag, gfp_t gfp)

        ...

    pfrag->offset = 0;
    if (SKB_FRAG_PAGE_ORDER) {
        /* Avoid direct reclaim but allow kswapd to wake */
        pfrag->page = alloc_pages((gfp & ~__GFP_DIRECT_RECLAIM) |
                                  SKB_FRAG_PAGE_ORDER);
        if (likely(pfrag->page)) {
            pfrag->size = PAGE_SIZE << SKB_FRAG_PAGE_ORDER;
            return true;
        }
    }

        ...
```

```
#define SKB_FRAG_PAGE_ORDER get_order(32768)
```

Technical Description

Vulnerability Root Cause

- Introduced in Linux Kernel by commit 03e2a30f6a27 (esp6) and commit cac2661c53f3 (esp4) in 2017

crypto/crypto_null.c

```
static int skcipher_null_crypt(struct blkcipher_desc *desc,
                               struct scatterlist *dst,
                               struct scatterlist *src, unsigned int nbytes)
{
    struct blkcipher_walk walk;
    int err;

    blkcipher_walk_init(&walk, dst, src, nbytes);
    err = blkcipher_walk_virt(desc, &walk);

    while (walk.nbytes) {
        if (walk.src.virt.addr != walk.dst.virt.addr)
            memcpy(walk.dst.virt.addr, walk.src.virt.addr,
                   walk.nbytes);
        err = blkcipher_walk_done(desc, &walk, 0);
    }

    return err;
}
```

Technical Description

Fix of the vulnerability

- Patch introduced in ebe48d368e97 [1]

[1] https://etenal.me/archives/1825

Technical Description

Fix of the vulnerability

- Patch introduced in ebe48d368e97 [1]

net/ipv6/esp6.c

```
@@ -490,6 +491,10 @@ int esp6_output_head(struct xfrm_state *x, struct sk_buff *skb, struct esp_info
                        return err;
        }

+       allocsz = ALIGN(skb->data_len + tailen, L1_CACHE_BYTES);
+       if (allocsz > ESP_SKB_FRAG_MAXSIZE)
+               goto cow;
+
        if (!skb_cloned(skb)) {
                if (tailen <= skb_tailroom(skb)) {
                        nfrags = 1;
```

[1] https://etenal.me/archives/1825

Source: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ebe48d368e97d007bfeb76fcb065d6cfc4c96645

Technical Description

Fix of the vulnerability

- Patch introduced in ebe48d368e97 [1]

```
--- a/include/net/esp.h
+++ b/include/net/esp.h
@@ -4,6 +4,8 @@

 #include <linux/skbuff.h>

+#define ESP_SKB_FRAG_MAXSIZE (PAGE_SIZE << SKB_FRAG_PAGE_ORDER)
+
```

[1] https://etenal.me/archives/1825

Source: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ebe48d368e97d007bfeb76fcb065d6cfc4c96645

Technical Description

Fix of the vulnerability

- Patch introduced in ebe48d368e97 [1]

```
--- a/include/net/esp.h
+++ b/include/net/esp.h
@@ -4,6 +4,8 @@

 #include <linux/skbuff.h>

+#define ESP_SKB_FRAG_MAXSIZE (PAGE_SIZE << SKB_FRAG_PAGE_ORDER)
+
```

32768 **4096** **3**

[1] https://etenal.me/archives/1825

Source: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ebe48d368e97d007bfeb76fcb065d6cfc4c96645

Proof of Concept

Exploit in order to get local privilege escalation [1]

1) Leak the KASLR offset.
    - Kernel Address Space Layout Randomization

[1] https://etenal.me/archives/1825

Proof of Concept

Exploit in order to get local privilege escalation [1]

1) Leak the KASLR offset.
   - Kernel Address Space Layout Randomization
2) Overwrite the path of modprobe.

[1] https://etenal.me/archives/1825

Proof of Concept

Exploit in order to get local privilege escalation [1]

1) Leak the KASLR offset.
   - Kernel Address Space Layout Randomization
2) Overwrite the path of modprobe.

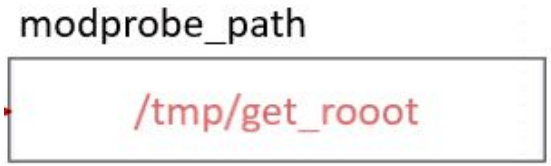
[1] https://etenal.me/archives/1825

Proof of Concept

Exploit in order to get local privilege escalation [1]

1) Leak the KASLR offset.
   - Kernel Address Space Layout Randomization
2) Overwrite the path of modprobe.

3) Trigger modprobe by running an unknown format file.



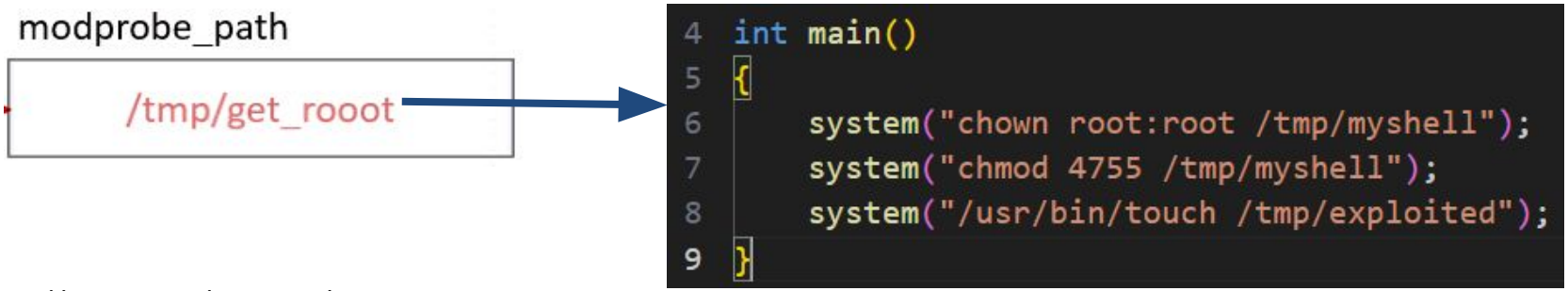
[1] https://etenal.me/archives/1825

Proof of Concept

Exploit in order to get local privilege escalation [1]

1) Leak the KASLR offset.
   - Kernel Address Space Layout Randomization
2) Overwrite the path of modprobe.

3) Trigger modprobe by running an unknown format file.




```
4  int main()
5  {
6      system("chown root:root /tmp/myshell");
7      system("chmod 4755 /tmp/myshell");
8      system("/usr/bin/touch /tmp/exploited");
9  }
```

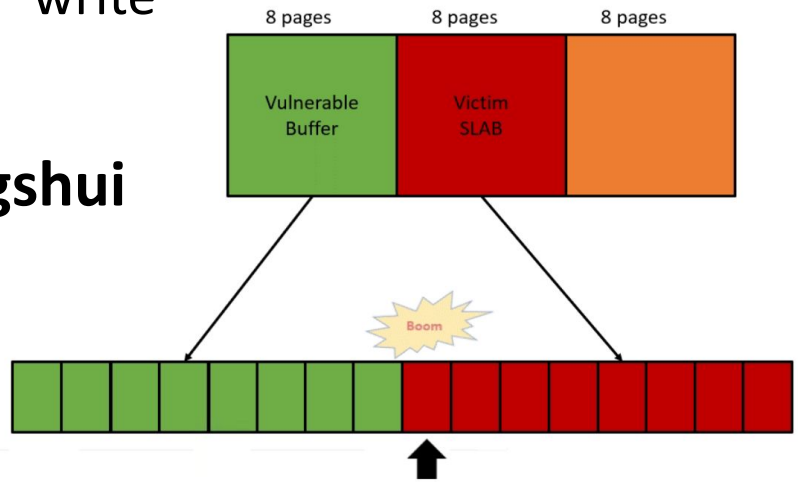
[1] https://etenal.me/archives/1825

Proof of Concept

Exploit in order to get local privilege escalation [1]

1) Leak the KASLR offset.
   - Kernel Address Space Layout Randomization
2) Overwrite the path of modprobe.

- **Page-level heap fengshui**



[1] https://etenal.me/archives/1825

Proof of Concept

Requirements

- Ubuntu Desktop 21.10 [1]

```
vboxuser@ubuntu-21:~$ cat /etc/issue
Ubuntu 21.10 \n \l
```

- 5.13.0-19-generic kernel version

```
vboxuser@ubuntu-21:~$ uname -a
Linux ubuntu-21 5.13.0-19-generic #19-Ubuntu SMP Thu Oct 7 21:58:00 UTC 2021 x8
6 64 x86 64 x86_64 GNU/Linux
```

[1] https://old-releases.ubuntu.com/releases/21.10/ubuntu-21.10-desktop-amd64.iso

CVE-2022-27666

-

Now, live demonstration

Guillermo Cruz Rojas
682433@unizar.es

Exploiting Software Vulnerabilities

Master's Degree in Informatics Engineering

Bibliography

IPsec

https://en.wikipedia.org/wiki/IPsec

CVE-2022-27666 (nvd.nist.gov)

https://nvd.nist.gov/vuln/detail/CVE-2022-27666

CVE-2022-27666 (exploit)

https://etenal.me/archives/1825

CVE-2022-27666

-

Questions

Guillermo Cruz Rojas
682433@unizar.es

Exploiting Software Vulnerabilities

Master's Degree in Informatics Engineering