CVE-2024-55587 - Zraniteľnosť knižnice libarchive umožňujúca Directory Traversal

Bezpečnostní analytici CSIRT.SK objavili zraniteľnosť v Python knižnici libarchive, ktorá umožňuje vykonávať útoky typu directory traversal.

Zraniteľné systémy:

- libarchive – 4.2.1

Vyššie uvedená verzia bola otestovaná. Nemôžeme vylúčiť, že zraniteľné sú aj staršie verzie.

Opis činnosti:

CVE-2024-55587

Zraniteľnosť sa nachádza v najnovšej verzii knižnice *libarchive* (4.2.1) a súvisí s absenciou ošetrovania názvov súborov nachádzajúcich sa v poskytnutom súbore ZIP. Táto zraniteľnosť sa nachádza v triede *ZipFile* v metódach *extract* a *extractall*. V prípade, že názvy súborov v nahranom súbore ZIP obsahujú relatívnu cestu (../) alebo aj absolútnu cestu (/tmp/test.txt) je možné danú zraniteľnosť zneužiť nasledovným spôsobom.

Keď napríklad vytvoríme súbor ZIP pomocou nasledovného Python kódu:

```
import pyzipper
import time

with pyzipper.ZipFile("exploit.zip", 'w', compression=pyzipper.ZIP_LZMA) as zf:
    current_time = time.localtime(time.time())[:6]
    zip_info = zf.zipinfo_cls(filename="/tmp/vulnerable.txt",  date_time=current_time)
    zf.writestr(zip_info, "vulnerable")
```

Vytvorí sa nám súbor ZIP s názvom *exploit.zip* obsahujúci jediný súbor s názvom */tmp/vulnerable.txt*.

Keď následne tento súbor extrahujeme za pomoci zraniteľnej metódy *extractall*:

```
from libarchive.zip import ZipFile

with ZipFile("exploit.zip",  mode="r") as archive:
    archive.extractall(path="./")
```

V adresári */tmp* sa nám vytvorí súbor s názvom *vulnerable.txt*, ktorý bude obsahovať text „vulnerable“.

Táto zraniteľnosť sa nachádza v súbore *libarchive/zip.py* na riadku 107:

```
return self.readpath(name, os.path.join(path, name))
```

kde premenná *name* nie je ošetrovaná. Vzhľadom na správanie metódy *join* v module *path* knižnice *os* teda novou cestou bude posledná zadaná absolútna cesta, t.j. nami zadaný názov súboru */tmp/vulnerable.txt*.
Zneužitím danej zraniteľnosti môže dôjsť napríklad ku získaniu prístupu na server prepísaním súboru *authorized_keys*, nachádzajúceho sa v podpriečinku *.ssh* domovského priečinku používateľa.

Zraniteľnosť bola overovaná s použitím nasledujúcich verzií knižníc:

- libarchive – 4.2.1

Možné škody:

- **Prepísanie citlivých súborov**

Odporúčania:

Pokiaľ pri vývoji webovej aplikácie v Python využívate knižnicu *libarchive* a používate metódu *extract* alebo *extractall* s použitím súboru ZIP, ktorý poskytol požívateľ, odporúčame zvážiť zmenu používanej knižnice na modernejšie alternatívy ako napríklad *pyzipper*.

Odkazy:

https://nvd.nist.gov/vuln/detail/CVE-2024-55587