Írásjogtól rootig AIX-on

Tanulmány

Silent Signal Kft.
Email: info@silentsignal.hu
Web: www.silentsignal.hu

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

Írásjogtól rootig AIX-on

1. Bevezető

A Silent Signal Kft. szakértői egy etikus hackelési projekt során felhasználói szintű távoli hozzáférést szereztek a Megbízó egy kritikus üzleti funkciót biztosító AIX kiszolgálójához. A kiszolgáló helyi biztonsági szintjének felmérése céljából, valamint a távolról kihasználható sérülékenység potenciális hatásának demonstrálása érdekében a szakértők kísérletet tettek a jogosultsági szint adminisztrátori (root) szintre történő emelésére. Számos elterjedt módszer sikertelen alkalmazása után a csapat több hiba együttes kihasználásával oldotta meg a problémát. Jelen dokumentum célja annak bemutatása, hogy az egyes biztonsági hiányosságok hogyan erősíthetik egymás hatását és vezetheznek teljes rendszer-kompromittációhoz. Természetesen a megbízáshoz kapcsolódó szerződésekkel összhangban e dokumentum nem tartalmazza a megbízó nevét, a bizalmas információk pedig eltávolításra illetve megváltoztatásra kerültek.

2. Korlátozott írási lehetőség root jogosultsággal

Az előzetesen megszerzett információk (felhasználónevek, jelszavak) alapján egy általános jogosultsággal rendelkező felhasználóval sikerült belépni a szerverre. A jogosultsági szint segítségével shell hozzáférést sikerült szerezni:

```
$ id;oslevel;ifconfig -a
uid=205([redacted]) gid=205([redacted]) groups=202([redacted])
5.2.0.0
en0: flags=5e080863,c0<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT,CHECKSUM_OFFLOAD(ACTIVE),PSEG,CHAIN>
        inet 192.168.10.41 netmask 0xffffff00 broadcast 192.168.10.255
         tcp_sendspace 262144 tcp_recvspace 262144 rfc1323 1
en1: flags=5e080863,c0<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT,CHECKSUM_OFFLOAD(ACTIVE),PSEG,CHAIN>
        inet [redacted] netmask 0xfffffc00 broadcast [redacted]
         tcp_sendspace 262144 tcp_recvspace 262144 rfc1323 1
en2: flags=5e080863,c0<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT,CHECKSUM_OFFLOAD(ACTIVE),PSEG,CHAIN>
        inet [redacted] netmask 0xffff0000 broadcast [redacted]
         tcp_sendspace 262144 tcp_recvspace 262144 rfc1323 1
en3: flags=5e080863,c0<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GROUPRT,64BIT,CHECKSUM_OFFLOAD(ACTIVE),PSEG,CHAIN>
        inet [redacted] netmask 0xfffffc00 broadcast [redacted]
         tcp_sendspace 131072 tcp_recvspace 65536
```

1. ábra. Kiinduló shell hozzáférés

A szerver AIX 5.2-es operációs rendszer futtatott. Az interneten megtalálható publikus biztonsági hiányosságok közül egyedül a CVE-2009-2669 jelű libc.a hiba működött a rendszeren. A sérülékenység segítségével bárki számára írható fájlokat lehetséges létrehozni root jogosultsággal, vagy meglévő fájlok tartalmát lehet módosítani, de ilyen esetben a tartalmat nem lehet befolyásolni a jogosultsági rendszer miatt. Ahogy a nyilvános exploit leírása is megemlíti, a sérülékenység általános módszerekkel, mint amilyen a .rhosts felülírása, vagy a dinamikus linker manipulálása nem használható ki - rendszerspecifikus támadási vektorra van tehát szükség.

3. Biztonsági funkció - Biztonsági rés

A szakértők a rendszer átvizsgálása után találtak egy scriptet az /etc/profile fájlban, amely a jelszavak lejárati időpontját ellenőrizte és értesítette a felhasználókat a jelszó változtatásra. Az üzemeltetők tehát igyekeztek gondot fordítani a jelszó-házirend betartatására, ami a vállalat biztonsági előírásainak egyik leglényegesebb eleme, mégis ez a fejlesztés tette végül lehetővé az előző pontban bemutatott sérülékenység teljesértékű kihasználását.

```
trap 1 2 3
sudo /usr/local/bin/pwlejar.sh $LOGNAME bbb

PATH=/usr/bin:$PATH     # SD Installer: do not remove !
export PATH     # SD Installer: do not remove !
#START===SDO_PROFILE_BLOCK_DO_NOT_CHANGE===START
```

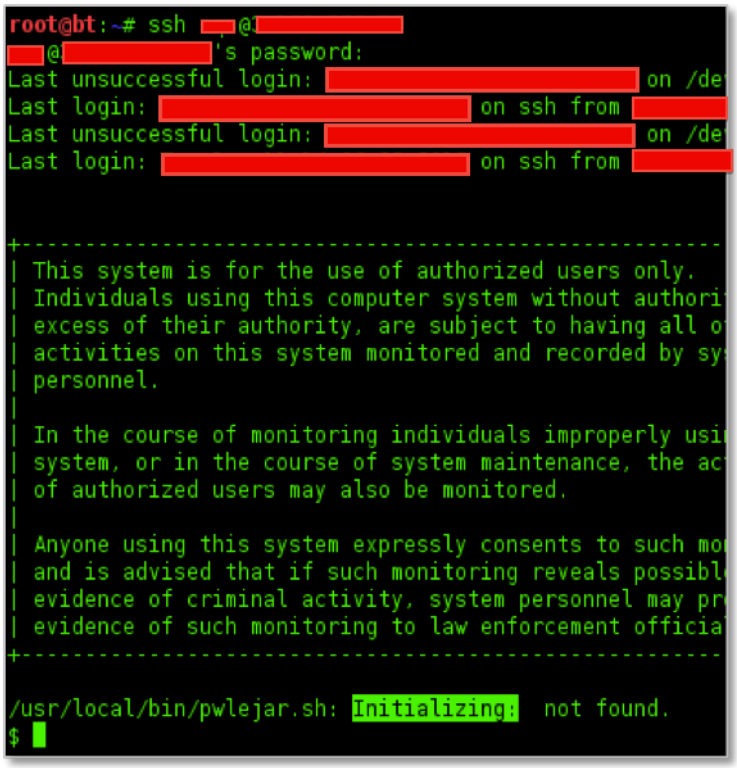
2. ábra. /etc/profile fájl részlete

Amint a fenti képen látható, a szkript sudo-n keresztül root jogosultsággal fut. A sudo konfigurációja ennek a szkriptnek a futtatását bármely felhasználó számára jelszó megadása nélkül lehetővé teszi:

```
if [ $# -lt 2 ]
  then echo A $user passwordje meg $maradek napig el
  else if [ $maxage -ne 0 ] && [ $maradek -gt 0 ] && [ $maradek -lt $pwwarn ]
         then
          echo "\t#############################################################"
          echo "\t# Figyelem a passwordje $maradek nap mulva lejar!!!\t\t#"
          echo "\t#############################################################"
           echo "\tUss barmit..."
           read a
        fi
fi
$ sudo /usr/local/bin/pwlejar.sh bbb
$
```

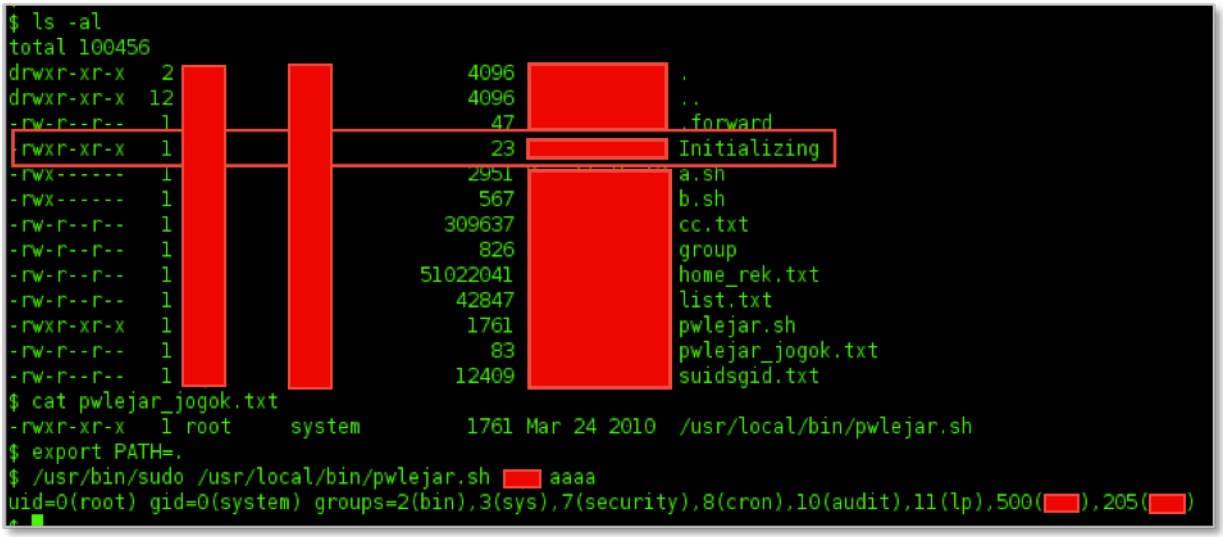
3. ábra. Futtathatóság ellenőrzése, nincs hibaüzenet

A libc.a biztonsági hiba segítségével felülírásra került az /usr/local/bin/pwlejar.sh, amelynek első szava az Initializing lett. Amennyiben futtatásra kerül ez a shell script a rendszer tájékoztatja a felhasználót, hogy nem találja az Initializing parancsot.



4. ábra. A rendszer nem találja az Initializing parancsot

A szakértők ezek után létrehoztak egy tetszőleges, de írható könyvtárban egy Initializing nevű futtatható shell scriptet, amely egy /usr/bin/id parancs végrehajtását tartalmazta. A hiba kihasználásához a PATH környezeti változó értékét kellett beállítani az aktuális könyvtárra, valamint meghívni a pwlejar.sh scriptet sudo-n keresztül.



5. ábra. A szakértők által definiált parancs root jogkörrel fut

Természetesen az id parancs ezek után tetszőleges más utasítással is helyettesíthető, az interaktív root shell megszerzése innentől kezdve magától értetődő.

4. Konklúzió

Kritikus folyamatokat futtató kiszolgálók esetén az operációs rendszer frissítése gyakran elmarad, mivel a szolgáltatás rendelkezésreállásának és hibamentes működésének igénye általában felülírja a javítócsomagoktól várt biztonsági kockázatcsökkenést. A bizonságtudatos üzemeltetők dolga még nehezebb, ha az első fejezetben tárgyalthoz hasonló, nehezen demonstrálható problémák javításának szükségességét kell megindokolni. A rendszeres biztonsági frissítések fontosságának hangsúlyozása ilyen értelemben tehát nem elég, de egy offenzív megközelítésű vizsgálat segíthet a javítások priorizálásában és a biztonsági szempontok érvényesítésében.

Megjegyzendő továbbá, hogy a biztonsági funkciók - legyen szó ismert biztonsági termékről, vagy belső fejlesztésről - megvalósítása, hasonlóan az egyéb rendszerkomponensekhez új sérülékenységeket vezethet be. Az ilyen típusú problémák hatása általában súlyos, hiszen a biztonsági funkciók általában magas jogosultsági szintet igényelnek. Fontos tehát, hogy biztonsági rendszereink vizsgálatára is hangsúlyt fektessünk az általuk védett komponensek mellet.