Incident Report – Access Control Failure

POC: Maleya Neal (SOC Analyst), Jamar Jones (Mgr)

Incident Type: Unauthorized Access and Misconfiguration

Affected System: Splunk

Incident Description: A Level 2 SOC Analyst granted a collegue access to Splunk for log analysis, however, an unsuspected configuration issue hindered the ability to search within Splunk. After establishing an SSH connection to the Splunk server, it was discovered that a Level 1 SOC Analyst had unintentionally modified the critical config.conf file, located within the /opt/splunk directory.

Solution:

Step I: Using the Linux OS, the command locate config.conf was used to locate file in the Splunk directory

```
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/home/fstack/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
```

Step II: To investigate further, the command “cd” was used to access the file “config.conf” and the command “ls -l” was used to view the file permissions. It was then confirmed that users, groups, and others have read, write, and execute permissions to this file.

```
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 223 Nov 22 21:23 config.conf
```

Step III: To verify the integrity of the file, md5sum was used. After admin permissions were updated to reflect Step IIIa, the file was again monitored for integrity.

```
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
96fb87fcf2f37541aebd17780a55eaf9  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ vim config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
4ea1a276c8210e60446ab59696146f42  config.conf
```

Step IIIa: To update access controls and ensure appropriate admin permissions, the command nano config.conf was used.

```
  GNU nano 4.8                          config.conf
[admin]
- AliceAdmin1
- MaleyaAdmin2
```

Incident Report – Access Control Failure

Step IV: Once the admins were updated, a backup copy of the “config.conf” was created in the /home/fstack directory.

```
fstack@ubuntu:/opt/splunk/etc/system/local$ cp config.conf /home/fstack
fstack@ubuntu:/opt/splunk/etc/system/local$ cd /
fstack@ubuntu:/$ cd /home/fstack
fstack@ubuntu:~$ ls
Desktop    InitialPackages.txt  Public     config.conf  nano.save  scripting
Documents  Music                Templates  demo1        practice   ubuntu
Downloads  Pictures             Videos     demo2        sample.sh
fstack@ubuntu:~$
```

Key Findings:

1. **Unauthorized Access:** Unauthorized access was granted to all users.

2. **Configuration Issue:** The incident was attributed to a misconfiguration in the Splunk configurations file, indicating a security lapse in the setup.

3. **Insecure Permissions:** Users, groups, and other entities were found to have excessive privileges on the Splunk configurations file, posing a security risk.

Impact:

1. **Data Exposure Risk:** Unauthorized access and insecure configurations elevate the risk of sensitive data exposure within Splunk.

2. **Operational Disruption:** The misconfiguration hindered the normal functioning of Splunk, impacting the ability to conduct necessary searches for security analysis.

Recommendations for Prevention:

1. **Regular Audits:** Conduct regular security audits to identify and rectify any misconfigurations or unauthorized access.

2. **Principle of Least Privilege**: Enforce the principle of least privilege to ensure that users have only the necessary access required for their roles

3. **Training and Awareness:** Conduct training sessions to enhance awareness among SOC analysts about the criticality of Splunk configurations and the potential impact of inadvertent changes

Conclusion: The incident highlights the critical importance of maintaining secure configurations and access controls to prevent unauthorized access and ensure the integrity of cybersecurity systems like Splunk. Immediate actions were taken to mitigate the risks, and preventive measures have been recommended to enhance the overall security posture.