Incident Report – Access Control Failure

*POC: Vijay Chola(SOC Analyst), Abhishek (Mgr)*

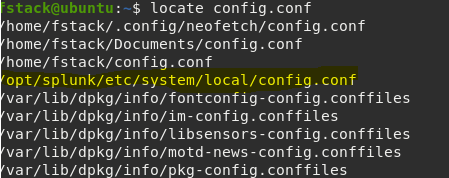
**Incident Type:** Unauthorized Access and Misconfiguraon

**Affected System:** Splunk

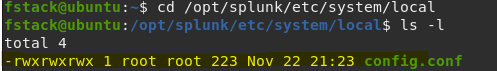
**Incident Descripon:** A Level 2 SOC Analyst granted a collegue access to Splunk for log analysis, however, an unsuspected configuraon issue hindered the ability to search within Splunk. Aer establishing an SSH connecon to the Splunk server, it was discovered that a Level 1 SOC Analyst had unintenonally modified the crical config.conf file, located within the /opt/splunk directory.

**Soluon:**

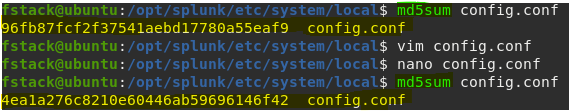
Step I: Using the Linux OS, the command locate config.conf was used to locate file in the Splunk directory



Step II: To invesgate 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.



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

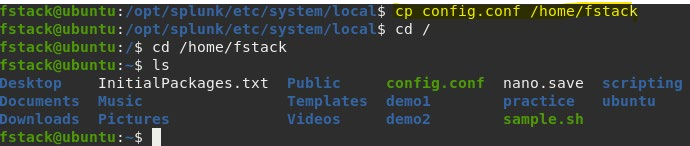


Step IIIa: To update access controls and ensure appropriate admin permissions, the command nano config.conf was used.



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.



**Key Findings:**

1. **Unauthorized Access:** Unauthorized access was granted to all users.
2. **Configuraon Issue:** The incident was atributed to a misconfiguraon in the Splunk configuraons file, indicang a security lapse in the setup.
3. **Insecure Permissions:** Users, groups, and other enes were found to have excessive privileges on the Splunk configuraons file, posing a security risk.

**Impact:**

1. **Data Exposure Risk:** Unauthorized access and insecure configuraons elevate the risk of sensive data exposure within Splunk.
2. **Operaonal Disrupon:** The misconfiguraon hindered the normal funconing of Splunk, impacng the ability to conduct necessary searches for security analysis.

**Recommendaons for Prevenon:**

1. **Regular Audits:** Conduct regular security audits to idenfy and recfy any misconfiguraons 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 cricality of Splunk configuraons and the potenal impact of inadvertent changes

**Conclusion:** The incident highlights the crical importance of maintaining secure configuraons and access controls to prevent unauthorized access and ensure the integrity of cybersecurity systems like Splunk. Immediate acons were taken to migate the risks, and prevenve measures have been recommended to enhance the overall security posture.