Security Report: Splunk Configuration File Permissions & Integrity

Prepared by: Afsheen Golanbar
Date: May 13, 2025
To: Jamar, Cybersecurity Manager

Executive Summary

While checking why Splunk wasn't letting me search logs, I found a serious issue: a file that controls how Splunk works (`config.conf`) was left wide open — anyone using the system could change it. That's risky.

There were two versions of this file. One was in my Documents folder, which is okay and likely just a test or backup. But the important one was deep inside the Splunk folder: `/opt/splunk/etc/system/local/config.conf`. That's the file Splunk uses directly to do its job. If someone messes with that file, it could confuse Splunk, stop it from collecting logs, or even create security holes.

This situation affects all three parts of the CIA security model:

- **Confidentiality**: Sensitive settings were visible to everyone.
- **Integrity**: Anyone could accidentally or intentionally change things.
- **Availability**: Splunk might stop working correctly.

To fix the problem, I made sure only system admins (like root) can touch that file. I also made a backup, checked the file's fingerprint before and after changes, and made sure it was safe.

Introduction

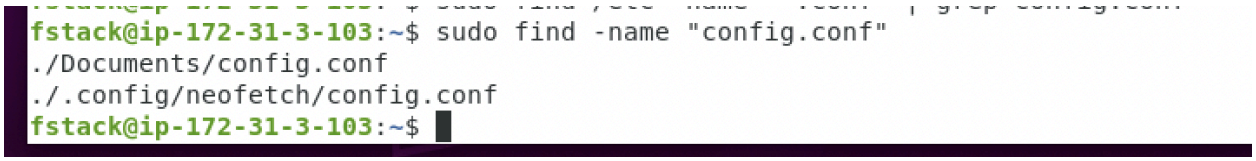
The purpose of this report is to document a configuration vulnerability found during Splunk log access troubleshooting. It highlights the potential security implications, corrective actions taken, and future preventative recommendations. This is part of StackFull Software's ongoing initiative to ensure proper security controls are in place for systems critical to incident detection and response.

Body

Problem Discovery

While attempting to investigate Splunk logs, I found I was unable to search or retrieve log data. This triggered an investigation into possible configuration issues. Using the `find` command, I identified that `config.conf` existed in multiple locations including:

- `/home/fstack/Documents/config.conf` (likely non-active local copy)
- `/opt/splunk/etc/system/local/config.conf` (active and critical)



Using `ls -l`, I reviewed the permissions of the active config file and discovered the following:

This shows the file was accessible for read, write, and execute operations by all users (world-writable and executable), representing a serious breach in **confidentiality** and **integrity**.

CIA Triad Justification

- **Confidentiality**: Any user on the system could read sensitive configurations.
- **Integrity**: Anyone could edit or corrupt the file, either maliciously or accidentally.
- **Availability**: Malicious modifications could break Splunk's ability to parse logs correctly, reducing availability of system insights.

Solution Implementation

To resolve the issue:

> I used `chmod 600 config.conf` to change file permissions so only the root user could read and write:

```
fstack@ip-172-31-3-103:/opt/splunk/etc/system/local$ sudo chmod 600 config.conf
fstack@ip-172-31-3-103:/opt/splunk/etc/system/local$ ls -l
total 4
-rw------- 1 root root 227 May  8 00:52 config.conf
fstack@ip-172-31-3-103:/opt/splunk/etc/system/local$
```

-rw------- 1 root root ... config.conf

I verified the file's MD5 hash using `md5sum` and saved the results in two separate files. The hash of the original file was saved in `conf.doc.txt`, and the hash after editing was saved in `cofedit.doc.txt`. This comparison confirmed the file's integrity before and after modification.

```
fstack@ip-172-31-3-103:~$ diff conf.doc.txt cofedit.doc.txt
1c1
< e5c5955c57d7b1d7672b60973a302b00  config.conf
---
> 8e1fce19e79f4bccf591933651ff96f8  config.conf
fstack@ip-172-31-3-103:~$
```

I edited the file using nano and appended the following block:

```
  GNU nano 4.8                        config.copy.conf

[inputs]
 - Windows logs
 - Firewall logs
 - Jira logs
 - Software engineering logs
 - IPS logs
 - IDS logs
 - WAF logs

[viewers]
 - Emily
 - Neel
 - James
 - Riley
 - Sarah
[admin]
   -AliceAdmin1
   -[Afsheen]Admin2
```

I backed up the final version to my home directory

```
fstack@ip-172-31-3-103:~$ ls
AFSHEEN    Public          config.copy.conf
Desktop    Templates       confing.edit.conf
Documents  Videos          confopt.doc.txt
```

cp /opt/splunk/etc/system/local/config.conf ~/config.edit.conf.

Monitoring and Recommendations

To prevent future unauthorized changes:

1. **Access Control**: Limit file modification to a trusted group of admins.
2. **Integrity Monitoring**: Use a daily cron job with `md5sum` to monitor changes and alert via email.
3. **Logging**: Enable audit logging on this directory to detect unauthorized access attempts.

Conclusion

This investigation revealed a critical misconfiguration that posed significant cybersecurity risks. Through proper file permission settings, integrity verification, and backup creation, the issue has been resolved. Ongoing monitoring and access control measures are recommended to ensure the long-term security and reliability of the Splunk system.
