Professional Security Enhancement Report: Splunk Configuration File Integrity
Prepared for: Executive Leadership
Date: February 28, 2025
Prepared by: Security Operations Team

I. Executive Summary

A critical vulnerability in Splunk's configuration file (config.conf) was identified, where unauthorized tampering disrupted log access for authorized personnel. This report details immediate remediation steps to secure the file, including access restrictions, integrity verification, and backup protocols. Implementation of these measures ensures compliance with confidentiality (CIA triad) requirements and prevents future operational disruptions.

II. Background Analysis

Issue: Unauthorized modifications to config.conf compromised Splunk's log access controls, violating:

- **Availability:** Authorized users (e.g., Alice, Hameed) lost access to logs.
- **Confidentiality:** Overly permissive file permissions allowed global read/write access.
- **Integrity:** No mechanism existed to detect tampering.

Objective: Secure the configuration file through permission hardening, integrity monitoring, and backup redundancy.

III. Steps Taken & Evidence

A. Locating the Configuration File

- **Command:** find /opt/splunk -name config.conf
- **Path Identified:** /opt/splunk/etc/system/local/config.conf

Purpose: Confirmed file location for targeted remediation.

B. File Permission Hardening

- **Initial Permissions:**
  rwxrwxrwx 1 splunk splunk 1.2KB Jul 30 18:40 config.conf # Global R/W/X access (high risk)
- **Remediation:**
  sudo chmod 700 /opt/splunk/etc/system/local/config.conf # Restrict to root-only access
  sudo chown root /opt/splunk/etc/system/local/config.conf # Assign root ownership

Outcome: Confidentiality enforced; only root can modify the file.

C. Baseline Integrity Verification

- **Initial MD5 Hash:** c70754d9c7bab08a8c441f90c37f27eb
- **Method:** md5sum /opt/splunk/etc/system/local/config.conf

Purpose: Established a trusted baseline for tamper detection.

D. Authorized Modification & Re-verification

- **Action:** Added Alice and Hameed to [Admins] group via vim.
- **Post-Modification Hash:** 0708706c550a14b4d9291247240cbd5b

Verification: Hash change confirmed legitimate update.

E. Backup Creation

- **Command:** cp /opt/splunk/etc/system/local/config.conf /home/fstack/
- **Purpose:** Ensured rapid recovery availability.

IV. Recommendations

1. **Access Control:**
   - Maintain chmod 700 and root ownership to limit modifications to authorized administrators.
2. **Integrity Monitoring:**
   - Implement scheduled md5sum checks (e.g., daily via cron job) and alert on hash mismatches.
3. **Backup Protocol:**
   - Store encrypted backups in a separate location.

V. Conclusion

The Splunk configuration file is now secured through least-privilege access, proactive integrity checks, and redundant backups. These measures ensure:

- **Confidentiality:** Only root can alter the file.
- **Integrity:** Tampering is immediately detectable via hash verification.
- **Availability:** Backups guarantee rapid recovery.

This framework aligns with industry best practices (NIST SP 800-53) and mitigates future operational risks.

APPENDIX

Post-Remediation Permission Sample:

- rwx------ 1 root root 1.2KB Jul 31 10:00 config.conf