Your Company

123 Your Street
Your City, ST 12345
(123) 456 - 7890

Addressing Cybersecurity Risk: Resolving Permissions Vulnerabilities in Third-Party Networks

May 23, 2024 By Edvin Morales

Overview

One of the main problems is permissions for third-party networks. This can cause bad actors to take advantage of our very loose permissions. This is posing a significant cybersecurity risk ! The report will detail these vulnerabilities, their potential impact , and the action taken to mitigate them.

Find Problem

I was unable to look at the logs from the splunk network. I looked for /opt/splunk due to all files being stored in this directory.

Key Findings

1.The file has read, write ,and execute privileges for anybody even when root is the owner

2.Unauthorized access to sensitive data due to incorrect permissions settings

3.Insufficient oversight on third-party access controls

```
fstack@ip-172-31-50-181:/opt/splunk/etc/system$ cd local
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
```

Recommendations

1. Implement stricter access control policies
2. Conduct regular permission audits
3. Enhance training programs for employees and providers

Details

Scope: This audit aims to shine a light on the permission problem with files. All the tools I used to find the permissions issue cd ,ls -l ,md5sum ,vim ,and cp.

Methodology: First I looked for the opt directory that houses software and add-on packages not a part of the default installation. After I found the splunk directory I looked for the config file

```
fstack@ip-172-31-50-181:/opt/splunk/etc/system$ cd local
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$ ls -l
total 4
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
```

I saw that the file had permissions open for everybody. I md5sum the file to get the unedited hash of the file. Then I vim the file to add another group with higher permissions.

```
#EDIT ME

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

[viewers]
 - Emily
 - Neel
 - James
 - Riley
 - Sarah
[admins]
 -AliceAdmin1
 -EdvinAdmin2
~
~
~
"config.conf" 20L, 222C
```

Then I checked the md5sum one more time to make sure I edited the file.

```
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$ md5sum config.conf
c70754d9c7bab08a8c441f90c37f27eb  config.conf
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$ vim config.conf
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$ md5sum config.conf
1e8000eb6253df75d78f189181ee0aa1  config.conf
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$
```

Finally I created a backup of the file to the home directory .

```
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$ cp config.conf /home/fstac
k/config.conf.backup
fstack@ip-172-31-50-181:/opt/splunk/etc/system/local$
```

Findings

Incident : Users were found to have excessive access privileges, far beyond what is necessary for their roles.

Impact : Increase risk of data leaks, misuse of data, and potential for insider threats

Discovery : Identified when trying to look at various logs in splunk

Risk Assessment

Impact Analysis:

1. High risk to data security and regulatory compliance due to unauthorized access
2. Medium to high risk to data misuse from excessive access privileges
3. Medium risk from insufficient oversight, leading to potential unnoticed vulnerabilities

Likelihood:

1. Medium likelihood of unauthorized access due to existing but flawed security measures
2. High likelihood of excessive access being exploited due to lack of regular audits
3. Medium likelihood of oversight issues leading to security incidents

Mitigation Strategies

Immediate Action Taken

- Revoked excessive access privileges from users
- Implemented immediate oversight enhancements to monitor access controls more effectively

Long-Term Recommendations

1. Access Control Policies:
    - Develop and enforce stricter access control policies, ensuring that permissions are granted based on the principle of least privilege.
2. Regular Audits:
    - Conduct regular, comprehensive audits of permissions settings and access logs to identify and rectify vulnerabilities promptly.
3. Training and Awareness:
    - Enhance training programs for employees and third-party providers to ensure they understand secure permissions management practices.

Oversight and Monitoring

Enhance Oversight: Established a more rigorous review process for third-party access controls, including quarterly reviews and real-time monitoring.

Continuous Monitoring:Implemented advanced monitoring tools to track permissions changes and access logs continuously, enabling prompt detection of unauthorized activities.

Conclusion

Addressing these permissions vulnerabilities is crucial for maintaining our cybersecurity posture. By taking immediate corrective actions and implementing long-term strategies, we can significantly mitigate risks and enhance our overall security.

Call to Action:

Stakeholders are urged to support and participate in the implementation of the recommended measures to ensure robust protection against permissions-related vulnerabilities.

Supporting Data:

- Detailed logs and screenshots of identified misconfigurations and access anomalies.

Glossary:

- Access Control Policies: Rules and guidelines that define who can access specific resources and under what conditions.
- Principle of Least Privilege: A security principle that states users should only have the minimum levels of access necessary to perform their job functions.