# Executive Summary

## Incident Overview

On 22nd September 2020, our jump host server experienced a security incident which was promptly detected through our monitoring systems. The attack involved unauthorized access and potential data compromise. Immediate action was taken to mitigate the threats and prevent further damage.

## Detection

The attack was identified at time range 10:52:51- 11:03:52 on 22-Sep-2020 through the Host-Based Intrusion Detection System HIDS. Indicators of compromise included attempts to login using a non-existent user, multiple failed login attempts, SSHD brute force  trying to get access to the system, missed passwords more than one time all followed by a successful authentication, addition of a new user and starting a new malicious service listening on a non-standard port and successful privilege escalation to root.

## Mitigation Actions

Upon detection, the following steps were taken to contain the threat:

1. **Isolation**: The affected server was isolated from the network to prevent further access.
2. **Investigation**: A thorough investigation was conducted to identify the nature and extent of the breach. This included:
    - Analyzing logs and system activities.
    - Identifying compromised accounts.
    - Performing Anti-Virus scans to some directories.
    - Assessing potential data exfiltration.
3. **Threat Neutralization**: Malicious files and unauthorized accounts were removed, and any backdoors were closed.

## Server Hardening and Preventive Measures

To enhance the security and prevent future incidents, several hardening measures were implemented:

- **Software and System Updates**: All software and operating systems were updated to the latest versions to patch known vulnerabilities.
- **Access Controls**:
    a. Implemented stricter access control policies.
    b. Enabled multi-factor authentication (MFA) for all administrative accounts.
    c. Reviewed and updated user permissions to ensure least privilege access.
- **Configuration Changes**:
    d. Configured security settings to hide Apache version and Linux OS information in HTTP headers.
    e. Disabled unnecessary services and ports.
    f. Configured the firewall to block unauthorized access and tuned a firewall rule to specifically block the attacker from accessing our server remotely.
    g. Configured SSH to deny remote access to root user
- **Monitoring Enhancements**:
    h. Improved logging and monitoring systems to detect suspicious activities more effectively and added a rule to detect the newly discovered threat.
    i. Set up automated alerts for unusual activities.
- **Regular Security Audits**: Established a routine for regular security audits and vulnerability assessments.

## Conclusion

The incident was swiftly detected and effectively mitigated, with no significant impact on operations. The comprehensive hardening measures implemented will strengthen our defenses against future attacks. Continuous monitoring and periodic security assessments will ensure ongoing protection.

Our commitment to cybersecurity remains a top priority, and we will continue to invest in advanced security measures to safeguard our infrastructure and data.

## Next Steps

1. **User Training**: Conduct security awareness training for all users to help them understand new policies and adhere to them.
2. **Incident Review**: A detailed review of the incident response will be conducted to identify any areas for improvement.
3. **Policy Update**: Update security policies and procedures based on lessons learned from the incident.