VoIP Incident Response Checklist

Date: Thursday 12th June 2025

Prepared by: Group H Security Team

---

1. Purpose

This playbook outlines the standardized procedures to detect, assess, contain, respond to, and recover from security incidents involving Voice over IP (VoIP) systems within the organization. It is designed to assist the Group H Security Team in ensuring prompt and effective handling of VoIP-related threats to protect confidentiality, integrity, and availability.

2. Scope

Applies to all VoIP communication systems, including but not limited to: - Asterisk servers - IP desk phones and softphones - SIP and RTP traffic - Session Border Controllers (SBCs) - Remote and mobile VoIP users

3. Roles and Responsibilities

Role	Responsibility
Incident Manager	Oversees response process and reporting
VoIP Engineer	Performs technical containment and restoration
Security Analyst	Conducts investigation and analysis
Communication Lead	Coordinates internal and external communications
IT Support	Assists in recovery and user notification

4. Incident Categories

Category	Description
Unauthorized Access	Use of stolen SIP credentials, unauthorized device registration

Category	Description
SPIT (VoIP Spam)	Mass unsolicited calls disrupting business functions
Call Interception	Eavesdropping or audio stream capture
Denial of Service (DoS)	SIP flooding, RTP disruption, or server overload
Configuration Breach	Misconfigurations leading to vulnerability exposure

5. Incident Response Lifecycle

5.1 Identification & Detection

- Continuous monitoring with IDS (Snort/Suricata) and VoIP logs
- Alerts for:
    - Multiple failed SIP REGISTER attempts
    - Sudden spike in INVITE messages
    - Abnormal call duration or destination
- Initial triage using SIEM alerts and correlation rules

5.2 Reporting & Notification

- Internal users report incidents via helpdesk or hotline
- IDS alert escalates to the Security Analyst
- Incident Manager initiates incident ticket and assigns roles
- Notify stakeholders and legal counsel if sensitive data is impacted

5.3 Containment

- Immediate actions:
    - Block offending IP via firewall
    - Suspend compromised SIP accounts
    - Isolate affected VoIP segment or VLAN
- Short-term measures:
    - Rate-limit SIP traffic
    - Disable auto-provisioning on exposed phones

5.4 Investigation & Analysis

- Collect:
    - Asterisk logs, call detail records (CDRs)
    - Packet captures (PCAPs) from SPAN port or IDS

    - Authentication logs, extension activity
- Analyze:
    - Root cause (vulnerability exploited, attacker IP, breach vector)
    - Lateral movement (other extensions affected?)

5.5 Eradication & Recovery

- Remove malicious IPs and sessions
- Patch vulnerable components
- Reset passwords and regenerate SIP secrets
- Restore services and test call integrity
- Verify TLS/SRTP is functioning and trusted certificates are in place

5.6 Communication & Documentation

- Prepare executive summary of incident
- Notify all affected users with instructions
- Document timelines, actions taken, tools used
- Maintain incident records in centralized system

5.7 Post-Incident Review

- Conduct review within 5 business days
- Identify gaps in detection or response
- Recommend improvements (e.g., new Snort rules, better monitoring)
- Update this playbook if necessary

6. Communication Plan

Audience	Method	Frequency	Responsible
Affected Users	Email	Once confirmed	IT Support
Executives	Report	Within 24h	Incident Manager
External Vendors	Phone/Email	If needed	Communication Lead

7. Tools and Resources

- IDS/IPS: Snort, Suricata
- Packet Capture: Wireshark
- SIEM Platform:[log manager]
- VoIP Server: Asterisk CLI, log monitoring tools
- VPN and Firewall: pfSense or equivalent
- Communication: Internal ticketing system, Slack, Email

8. Review and Maintenance

- The playbook must be reviewed annually or after every major incident.
- Changes require approval from the Head of Security.
- Latest version must be stored in the organization's security document repository.

Approval:
Name: __G8ST Management_____
Title: _____
Signature: _____
Date: __ 12TH June 2025_____