Incident Response Report

Executive Summary

On 2025-09-26, a high-severity security incident involving the exploitation of a legacy Samba service was detected. An external threat actor (IP: 192.168.1.108) leveraged the known usermap_script vulnerability (MITRE T1210) to gain unauthorized access and execute arbitrary code. The incident was detected by Wazuh and contained within minutes using an automated TheHive/CrowdSec playbook. No sensitive data loss was confirmed, but the root cause analysis revealed a critical failure in patch management processes for legacy systems.

Timeline

- 16:00:00 IST: Attacker initiates exploitation of Samba service.
- 16:01:05 IST: Wazuh/Elastic Security generates high-severity alert. (Detection)
- 16:02:30 IST: TheHive case created; Automated SOAR playbook triggered. (Triage & Response Start)
- 16:03:15 IST: CrowdSec blocks the attacker IP (192.168.1.108). Ping test verifies containment. (Containment)
- 16:04:00 IST: Incident resolved and investigation begins.

Root Cause Analysis (RCA)

5 Whys (Root Cause Analysis)

1. Why did the attacker gain access?
   - *Because* the attacker successfully executed code via the Samba service.
2. Why was the Samba service vulnerable?
   - *Because* the system was running an unpatched version with the usermap_script vulnerability.
3. Why was the software unpatched?
   - *Because* the Patch Management Process for this specific server was non-existent or insufficient.
4. Why was the patch management process insufficient?
   - *Because* there was no clear Asset Inventory or Vulnerability Scanning schedule for this legacy server.
5. Why was there no clear inventory/schedule? (Root Cause)
   - *Because* of a lack of organizational mandate and resources for comprehensive security maintenance on non-production/legacy systems.

Recommendations

1. Immediate Patching: Immediately patch or decommission all servers running vulnerable Samba versions.
2. Asset Inventory: Establish a complete and regularly audited asset inventory.
3. Vulnerability Management: Implement weekly automated vulnerability scanning and a mandatory patch management cadence for all assets.
4. Network Segmentation: Isolate legacy systems into a highly restricted network segment.