CYART

inquiry@cyart.io

www.cyart.io

Incident Response Report

1. Executive Summary

On December 19, 2025, a high-severity security incident was detected involving the exploitation of a vulnerable Samba service on a Metasploitable2 system. An attacker originating from IP address 10.0.2.19 leveraged the Samba usermap script vulnerability to achieve unauthorized remote command execution. The activity was detected by Wazuh, mapped to MITRE ATT&CK technique T1210, and confirmed as a true positive during alert triage. Immediate response actions were taken, including isolating the affected virtual machine and blocking the attacker's IP address using CrowdSec. The incident was escalated to L2 via TheHive for further analysis. No evidence of lateral movement or data exfiltration was observed.

Timestamp	Source IP	Alert Description	MITRE
2025-12-19 01:33:00	10.0.2.19	Samba usermap script exploitation detected	T1210

Table 1: Detection & Alerting

2. Timeline

Timestamp	Event
2025-12-19 01:30:00	Attacker initiated Samba exploitation attempt
2025-12-19 01:33:00	Wazuh generated high-severity alert for Samba exploit
2025-12-19 01:35:00	Alert triaged and confirmed as true positive
2025-12-19 01:38:00	Compromised VM isolated from the network
2025-12-19 01:39:00	Attacker IP blocked via CrowdSec
2025-12-19 01:40:00	Containment verified through failed ping test
2025-12-19 01:42:00	Incident escalated to L2

Table 2: Timeline

3. Impact Analysis

The attacker successfully gained a remote shell on the affected system, indicating full system compromise at the operating system level. Due to the controlled lab environment and rapid containment, the impact was limited to a single vulnerable virtual machine. No sensitive data was accessed, modified, or exfiltrated. There was no evidence of persistence mechanisms, privilege escalation beyond the initial exploit or lateral movement to other systems. Although the incident occurred in a test environment, similar exploitation in a production system could result in data breaches, service disruption or further network compromise if left undetected.

4. Remediation Steps

- Isolated the compromised VM from the network immediately.
- Blocked the attacker's IP address (10.0.2.19) using CrowdSec enforcement.
- Disabled the vulnerable Samba usermap script configuration.
- Recommended upgrading or patching the Samba service to a secure version.
- Reviewed Wazuh detection rules and confirmed MITRE mapping.
- Documented and escalated the incident to Tier 2 using TheHive.
- Recommended regular vulnerability scanning and patch management.

5. Lessons Learned

This incident demonstrated the importance of continuous monitoring and timely alert triage in detecting exploitation of exposed services. Proper integration of SIEM like Wazuh, response tooling like CrowdSec, and case management like TheHive enabled fast containment and escalation. The exercise highlighted the risk posed by unpatched services and misconfigurations. Regular SOC simulations, improved detection rules, and proactive vulnerability management are essential to reduce response time and minimize the impact of real-world attacks.