Incident Response Report

1. Executive Summary

On 12 December 2025, the SEIM (Wazuh) detected a malicious exploitation attempt targeting the vulnerable VSFTPD 2.3.4 service running on the victim machine (10.0.2.19). The attack originated from IP address 10.0.2.19, which attempted to trigger the known backdoor vulnerability using an FTP connection. The attack was identified, triaged, contained, and mitigated with no system compromise or service disruption. CrowdSec was used to immediately block the attacker's IP, and the affected machine was isolated to prevent further attempts. This incident demonstrates the effectiveness of the detection-and-response workflow and highlights key areas for strengthening defense.

2. Timeline

Time (IST)	Event Description
2025-12-12 20:00:00	Exploit attempt initiated from 10.0.2.19 targeting VSFTPD 2.3.4 on 10.0.2.18.
2025-12-12 20:00:00	Wazuh generates an alert for "VSFTPD 2.3.4 backdoor triggered."
2025-12-12 20:03:00	SOC analyst validates the alert and maps it to MITRE Technique T1190 – Exploit Public-Facing Applications.
2025-12-12 20:05:00	Investigation confirms malicious exploitation attempt.
2025-12-12 20:06:00	CrowdSec ban applied: 10.0.2.19 blocked for 4 hours.
2025-12-12 20:08:00	Ping test from attacker to victim fails, proving containment successful.
2025-12-12 20:10:00	Victim VM isolated for further review.

Table 1: Timeline

3. Impact Analysis

- The exploit attempt targeted a known vulnerability in VSFTPD 2.3.4, which contains an embedded backdoor that can grant unauthorized shell access.
- No successful compromise occurred; Wazuh detected the attempt before the payload stage.
- No data loss, service disruption, or unauthorized access was observed.
- If successful, the attacker could have gained root-level access, posing a high risk to system integrity and confidentiality.
- The incident confirms that exposed outdated services remain high-value targets for attackers.

4. Remediation Steps

Immediate Containment

- Blocked attacker IP (10.0.2.19) via CrowdSec firewall bouncer.
- Isolated victim VM from the network to prevent lateral movement.

System Hardening

- Removed or disabled VSFTPD 2.3.4 service from the system.
- Applied security patches and updated all relevant packages.
- Restricted access to unused ports and services.

Monitoring Enhancements

- Enabled additional Wazuh FTP related rules for granular detection.
- Verified CrowdSec bouncer automation for real-time blocking.

Validation

- Re-ran vulnerability scans to ensure no additional exposures.
- Confirmed that no backdoor shells or malicious accounts were created.

5. Lessons Learned

- Legacy services pose critical risks and should never be left enabled without strict need and hardening.
- Continuous monitoring is essential, as early detection prevented the attacker from gaining a foothold.
- Automated response tools (Wazuh and CrowdSec) significantly reduce reaction time and limit potential damage.
- Regular patching and vulnerability assessments must be part of routine maintenance, particularly for public-facing or network-accessible services.
- Improved documentation and playbooks help responders act quickly and consistently during incidents.

6. Stakeholder Briefing

A security incident occurred when an external system attempted to exploit a vulnerable FTP service on one of our test machines. Our monitoring tool, Wazuh, detected the activity immediately and alerted the team. After confirming the event, we isolated the affected system and used CrowdSec to block the attacker’s IP address, preventing any further access. No data was compromised, and the attempted intrusion was contained quickly. This incident highlights the importance of keeping older services updated and maintaining continuous monitoring. Additional recommendations have been provided to reduce similar risks going forward.