## INCIDENT REPORT – USE CASE 6
## Vulnerability Detection (Ubuntu Agent)

Incident ID: SOC-VULN-006
Incident Title: Detection of Known Software Vulnerabilities on Ubuntu Host
Date & Time: Jan 19, 2026 @ 10:53:00
Detection Source: Wazuh SIEM – Vulnerability Detection Module

**Affected Asset**
Host: Ubuntu Agent
Asset Type: Linux Server
Operating System: Ubuntu Linux
Severity: Medium

**Incident Summary**
Wazuh SIEM identified known security vulnerabilities on an Ubuntu Linux system by analyzing installed software packages and correlating them with published CVE data. The detected vulnerabilities represent potential security risks that could be exploited by attackers if remediation actions are not taken.

**Detection Details**
Detection Tool: Wazuh SIEM
Detection Type: Host-based Vulnerability Detection
Detection Module: Vulnerability Detector
Affected Package: Ubuntu system package
Installed Version: Outdated version detected
CVE ID: CVE-XXXX-XXXX (example)
CVSS Severity: Medium

**Investigation and Analysis**
Reviewed the vulnerability alerts displayed in the Wazuh dashboard and examined the affected package details, including the installed version, fixed version, and associated CVE information. The analyst assessed whether the vulnerable package was actively running and whether the system was exposed to external access. Correlation was performed with other security events, including authentication logs, command execution alerts, and network activity. No indicators of active exploitation were identified during the investigation.

**Classification**
True Positive – Security Exposure (No Active Exploitation Observed)

**Root Cause**
The Ubuntu system was running outdated software packages due to pending security updates, resulting in known vulnerabilities being present on the host.

**Impact Assessment**
No service disruption was observed.
No evidence of system compromise or exploitation was detected.
If left unpatched, the vulnerabilities could be exploited to gain unauthorized access or escalate privileges.

**Response Actions**
The vulnerability findings were documented and reported to the system owner.
Security updates and patching of affected packages were recommended.
Temporary mitigation measures were suggested where immediate patching was not feasible.
The system was placed under continued monitoring for signs of exploitation.

**Lessons Learned**

Regular vulnerability detection and timely patch management are essential to reduce the attack surface of Linux systems. Early identification of vulnerabilities allows SOC teams to take preventive actions before attackers can exploit known weaknesses.

**MITRE ATT&CK Mapping**

Tactic: TA0001 – Initial Access
Technique ID: T1190
Technique Name: Exploit Public-Facing Application
Technique ID: T1068
Technique Name: Exploitation for Privilege Escalation

**Incident Status**

Closed – Informational (Vulnerability Identified, Remediation Recommended)