# Vulnerability Analysis & Remediation Case Study

wazuh.

*Author: A. Brito*

*Date: February 2026*

## *Disclaimer:*

*This project is a simulated vulnerability management case study developed for professional portfolio purposes. While real vulnerability detection data was analyzed, all device names, hostnames, IP addresses, and identifying details have been edited, modified, or partially censored to preserve privacy and confidentiality. Any resemblance to actual production environments is generalized for demonstration purposes only.*

## *Executive Summary*

A 30-day vulnerability assessment was conducted across a simulated 20-endpoint SMB environment using Wazuh Vulnerability Detection. Initial analysis identified 155 total vulnerabilities, with a single Windows 11 Pro workstation accounting for 120 findings (77% of total exposure).

Targeted remediation reduced the endpoint's vulnerability count from 120 to 4 (96.6% reduction), eliminating the majority of High-severity findings and significantly decreasing overall organizational exposure.

## *Environment Overview*

- 20 endpoints (Windows and macOS)
- Wazuh v4.14.1 with Vulnerability Detector enabled
- OpenSearch dashboards for visualization
- 30-day analysis window

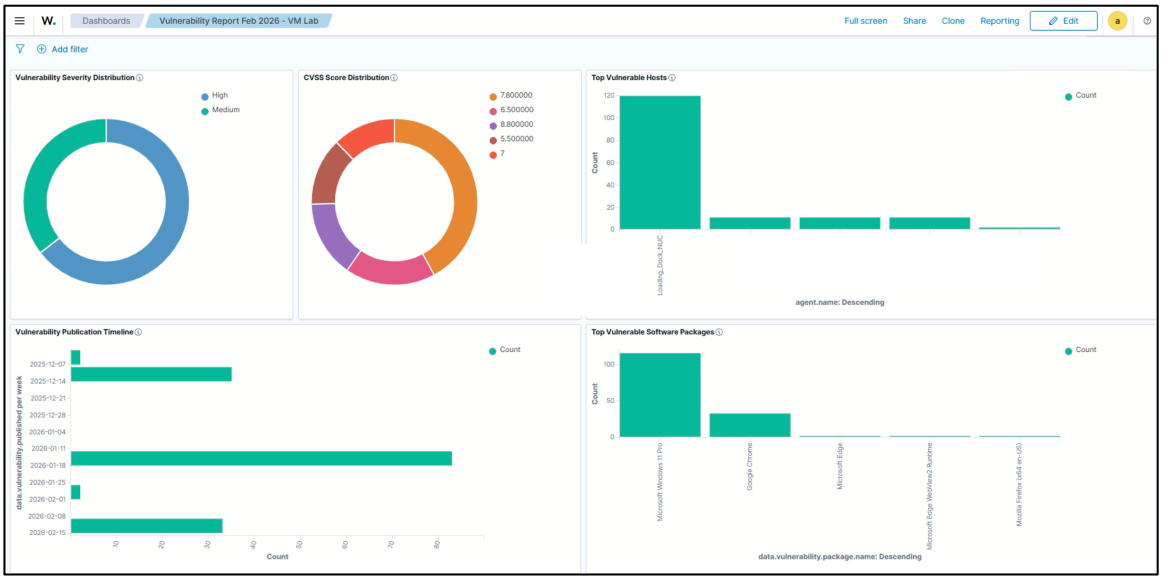


***Figure 1 – Baseline Vulnerability Dashboards***

*Wazuh Vulnerability Detection dashboard displaying severity distribution, CVSS score breakdown, vulnerability publication timeline, top vulnerable hosts, and top affected software packages over a 30-day analysis window.*

## *Phase 1: Baseline Vulnerability Assessment*

Query Used: *rule.groups: vulnerability-detector* (Last 30 Days)

**Findings:**

- 155 total vulnerabilities
- 69% of findings were classified as High severity
- One Windows 11 endpoint responsible for 120 findings
- 77% organizational exposure concentrated on one asset

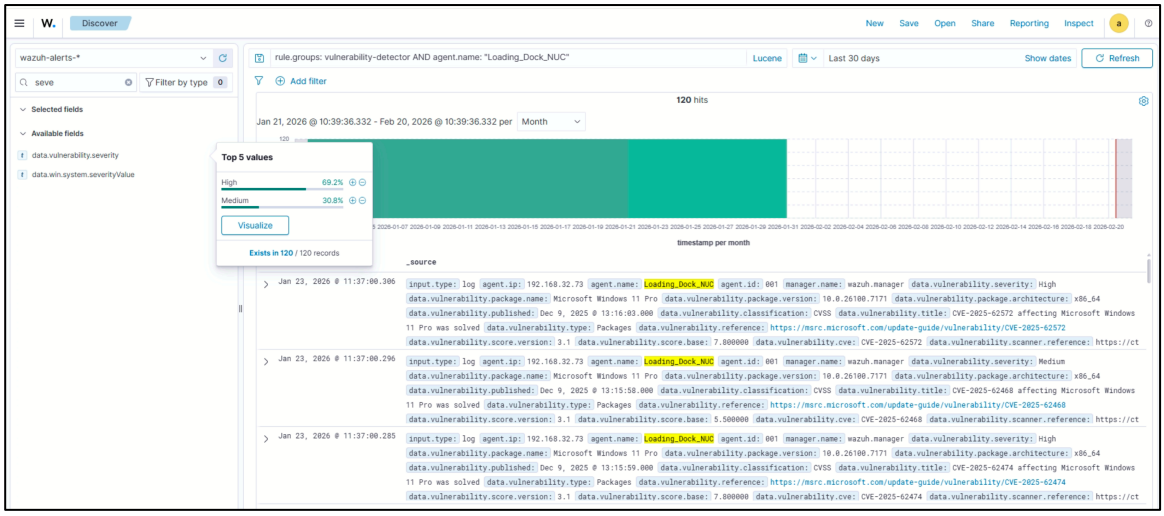


*Figure 2 – Initial Search*

## *Phase 2: Targeted Remediation*

Remediation actions included applying Windows cumulative updates, updating Microsoft Edge, rebooting the system, and restarting the Wazuh agent to trigger re-evaluation.

Post-remediation inventory results:

- 2 Critical
- 2 High
- 0 Medium
- 0 Low
- 96.6% vulnerability reduction on the targeted endpoint

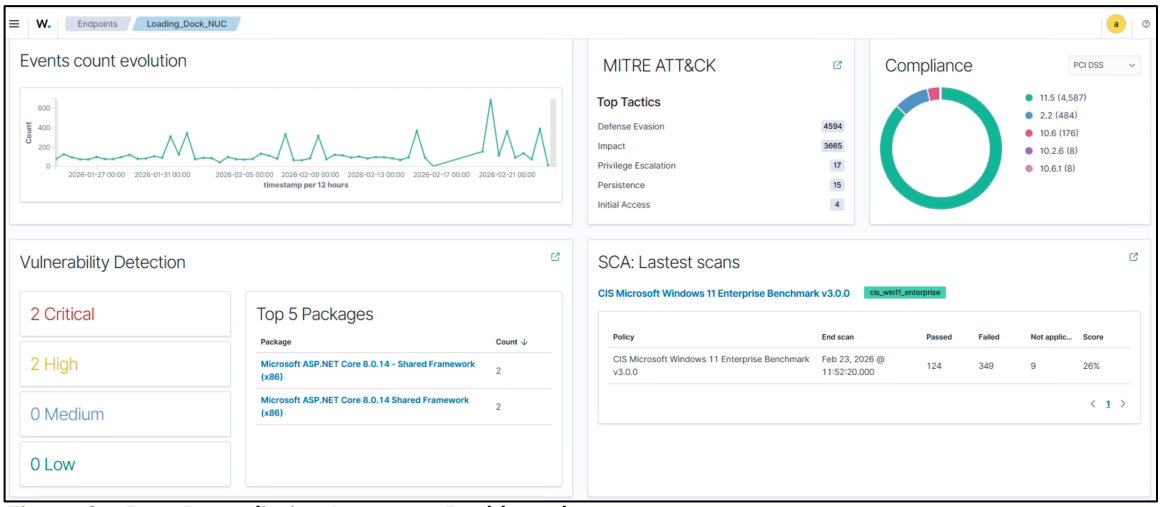


*Figure 3 – Post Remediation Inventory Dashboard*

## *Phase 3: Third-Party Runtime Remediation*

Remaining vulnerabilities were traced to an outdated ASP.NET Core 8.0.14 (x86) runtime (CVE-2025-55315). This demonstrated the need for third-party patch management beyond standard OS updates.

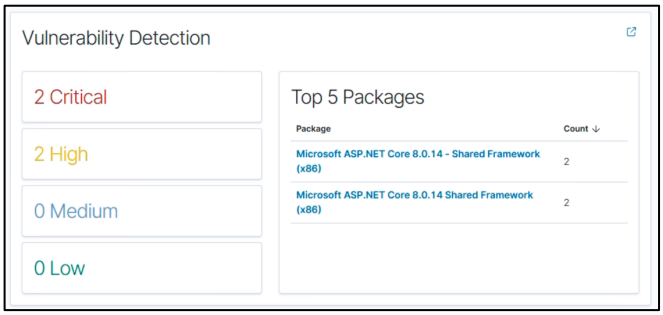


*Figure 4 – Remaining Vulnerabilities*

The runtime was updated to the latest 8.0.24 version, followed by system reboot and revalidation.

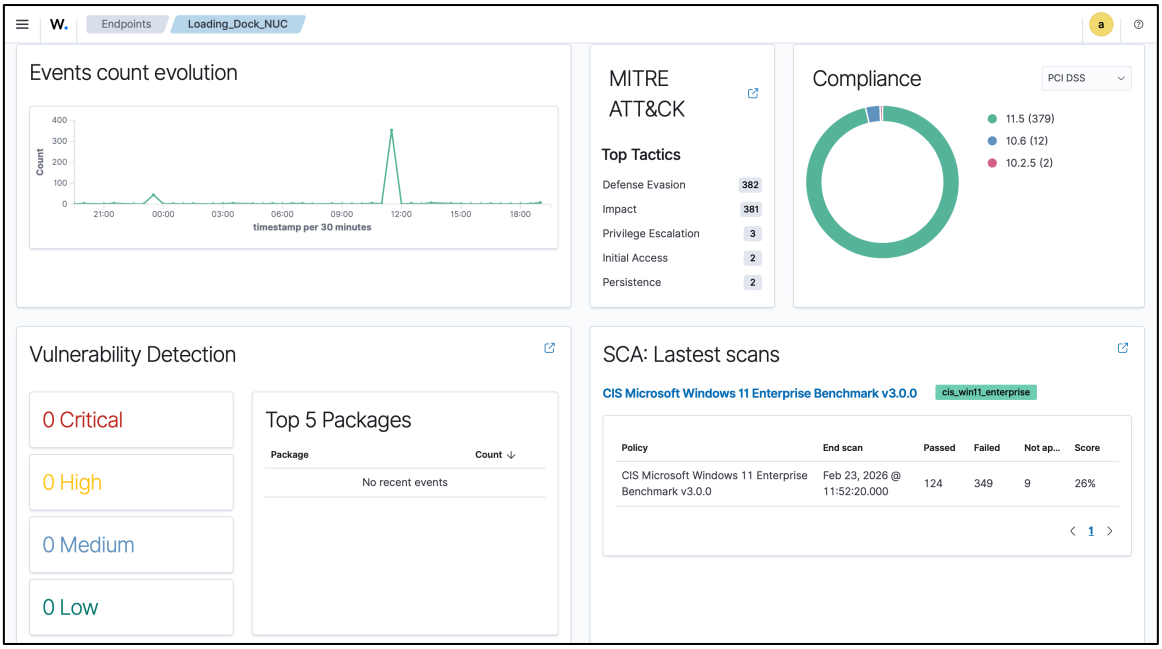


*Figure 5 – Post Runtime Patch Inventory Dashboard*

## *Lessons Learned*

- Vulnerability exposure is often highly concentrated on a small subset of assets.
- OS patching alone does not eliminate third-party runtime vulnerabilities.
- Inventory-based validation provides more reliable remediation confirmation than event logs alone.
- Quantified exposure reduction (percentage-based) demonstrates measurable risk impact.