

# Executive Summary

## Overview

This report provides a risk-focused overview of the enterprise vulnerability posture, highlighting current exposure, remediation performance, and key areas requiring leadership attention. Detailed operational metrics are available in the Vulnerability Risk Dashboard; this report is intended to support executive decision-making.

It is designed to help leadership prioritize resources, guide strategic risk mitigation, and ensure alignment with organizational security objectives.

## Key Messages for Leadership

- Vulnerability detection coverage is strong, with the majority of assessed CVEs actively identified.
- Risk exposure is concentrated in a smaller subset of Critical and High vulnerabilities.
- Many high-severity vulnerabilities are not being fixed within target timelines, which suggests that fixing them is the challenge — not finding them.
- As we find more vulnerabilities, our ability to reduce risk will not improve unless we change how we prioritize and set realistic timelines / SLAs.

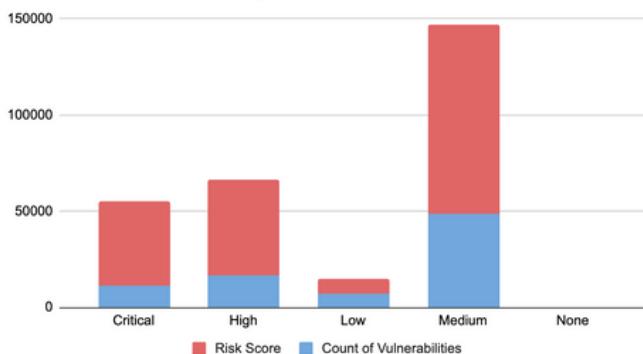
## Key Findings and Implications

### Detection and Visibility

- Detection rates indicate mature scanning coverage.
- Residual “not detected yet” vulnerabilities represent future exposure, not immediate failure.

We are already good at finding vulnerabilities. The bigger challenge now is deciding what to fix first and fixing the most important issues faster.

Current Snapshot	
Total CVEs Assessed	~ 89K
Detected Vulnerabilities	~ 94%
Critical + High (% of detected)	~ 33%
SLA Breach – Critical + High	> 90%
Aggregate Risk Score	Elevated



### Risk Concentration

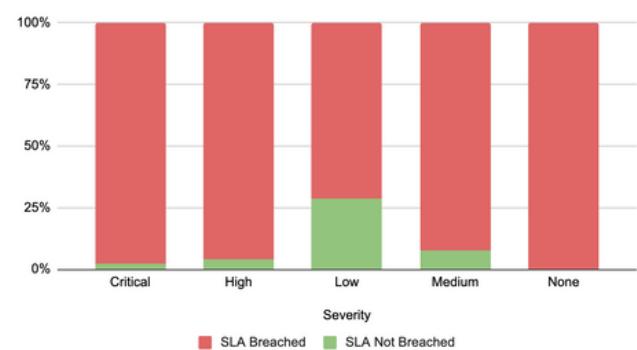
- Critical and High vulnerabilities, while fewer in number, drive disproportionate risk.
- Medium and Low vulnerabilities dominate volume and backlog but have lower individual urgency.

If teams focus on closing the largest number of vulnerabilities, they may spend too much time on lower-risk issues and not enough time on the ones that matter most.

### SLA Performance

- High SLA breach rates for Critical and High vulnerabilities suggest capacity and policy mismatch.
- Uniform SLA application does not fully reflect asset criticality, remediation complexity, or compensating controls.

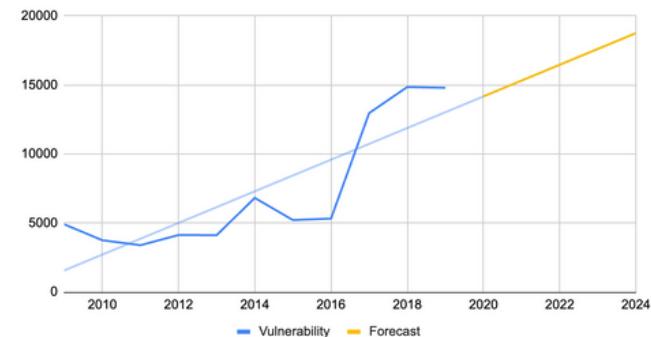
High SLA breach numbers may make performance look worse than it actually is, because timelines do not reflect how difficult some fixes are or how important each system is.



## Trend Analysis & Forecast

- The number of reported vulnerabilities increases steadily over time.
- The overall risk score also rises year over year, not just the total count.
- Growth appears to be driven by a combination of:
  - More software and systems in use
  - Increased discovery of vulnerabilities
  - Improved scanning and reporting capabilities

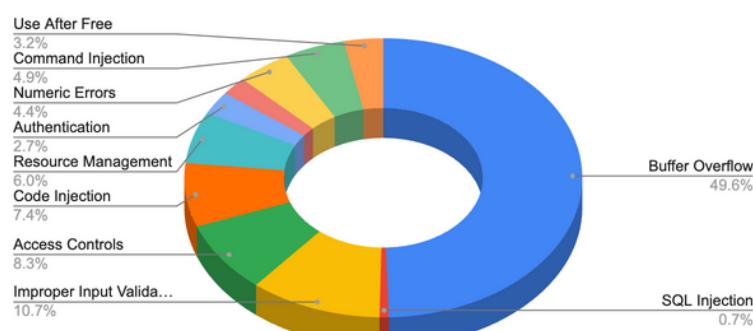
If current remediation and prioritization approaches remain unchanged, vulnerability backlog and risk exposure are likely to continue growing.



## Top 10 Vulnerability Categories - CWE

- A small number of vulnerability categories appear repeatedly across the dataset.
- High and Critical vulnerabilities are concentrated in a few recurring weakness types.
- These weaknesses are often related to:
  - Input validation
  - Access control
  - Memory handling
  - Authentication and authorization

Vulnerabilities are not random; the same types of issues occur repeatedly.



## Recommended Actions and Expected Outcomes

### 1. Refine SLA and Prioritization Model

Adopt a risk-based SLA framework that considers severity, asset criticality, and remediation feasibility.

#### Expected Outcome:

- More meaningful SLA metrics
- Reduced perceived breach inflation
- Clearer accountability

### 3. Reduce Repeat Vulnerabilities

Focus on fixing the most common types of weaknesses so the same problems do not keep coming back.

#### Expected Outcome:

- Fewer vulnerabilities over time
- Less work spent fixing the same issues again and again

### 2. Protect Capacity for P1 and P2 Remediation

Explicitly reserve remediation capacity for Critical and High (P1/P2) vulnerabilities to prevent distraction by high-volume P3 backlog.

#### Expected Outcome:

- Faster reduction of high-impact exposure
- Improved alignment between priorities and outcomes

### 4. Improve How Results Are Reported to Leaders

Use the dashboard for regular tracking, and use short executive reports to explain what the numbers mean and what actions leaders need to take.

#### Expected Outcome:

- Clearer understanding of risk
- better leadership decisions

## Conclusion

This assessment indicates that vulnerability risk is well-understood but unevenly reduced. Targeted prioritization, SLA refinement, and governance alignment are required to translate visibility into sustained risk reduction.