Vulnerability Analysis Dashboard

1. Executive KPIs

Total CVEs Assesed: 89660

Detected: 93.57%

Not Detected Yet: 6.43%

Total Detected: 83894

Severity — High + Critical: 32.98%

Critical: 13.18%

High: 19.80%

Detected Severity — Critical + High: 27669

SLA Breached — Critical + High: 96.60%

SLA Breached — Critical: 39.03%

SLA Breached — High: 57.57%

Total Risk Score: 199191

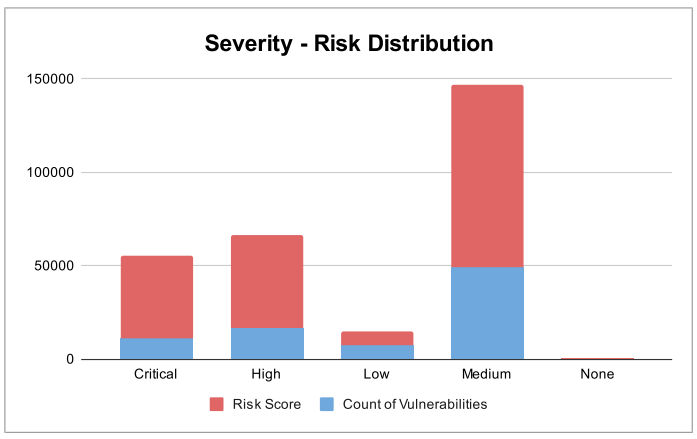
- Detection coverage is high, ~93% => strong visibility across assets. Small % contributes to latent risk.
- One third of the total vulnerabilities contribute to Critical and High severity; most breached SLAs are for High severity.

2. Severity Distribution (Risk Concentration)

Filter Used	Exposure_status=detected		
severity_v4	COUNTA of cve_id	COUNTA of cve_id	SUM of risk_v
Critical	11060	13.18%	44240
High	16609	19.80%	49827
Low	7324	8.73%	7324
Medium	48900	58.29%	97800
None	1	0.00%	0
Grand Total	**83894**	**100.00%**	**199191**

Insights:

Critical and High vulnerabilities represent 32% of all CVEs
=> Risk-based prioritization is needed rather than volume based; more focus required on critical and high severity exposure.



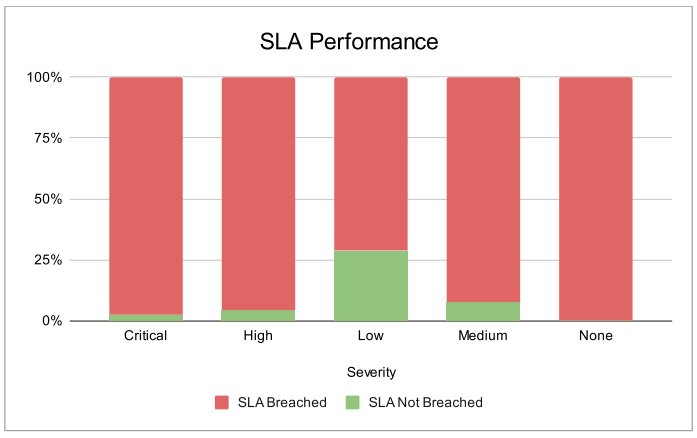
3. SLA Performance Breakdown

Filter Used	Exposure_status=detected		
COUNTA of cve_id	*SLA_breached*		
severity_v4	0	1	Grand Total
Critical	261	10799	11060
High	679	15930	16609
Low	2119	5205	7324
Medium	3727	45173	48900
None		1	1
Grand Total	**6786**	**77108**	**83894**

Insights:

High severity vulnerabilities represent the largest bottleneck.
=> Remediation efforts should be focused more on these

Uniform SLA for each severity, e.g. same SLA for all Critical, may be contributing to the large number of breached SLAs.
=> Have less aggressive SLAs as per the bandwidth, focus on historical backlogs

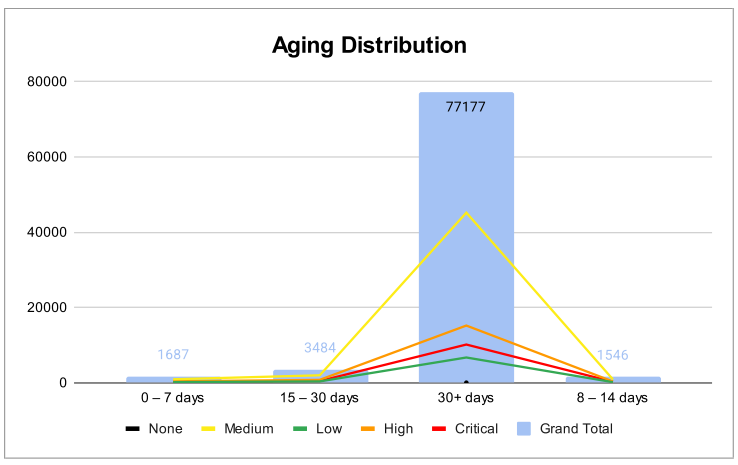


4. Aging Distribution

Filter Used	Exposure_status=detected					
COUNTA of cve_id	*severity_v4*					
age_bucket	Critical	High	Low	Medium	None	Grand Total
0 – 7 days	261	363	157	906		1687
15 – 30 days	434	753	337	1960		3484
30+ days	10135	15177	6691	45173	1	77177
8 – 14 days	230	316	139	861		1546
Grand Total	**11060**	**16609**	**7324**	**48900**	**1**	**83894**

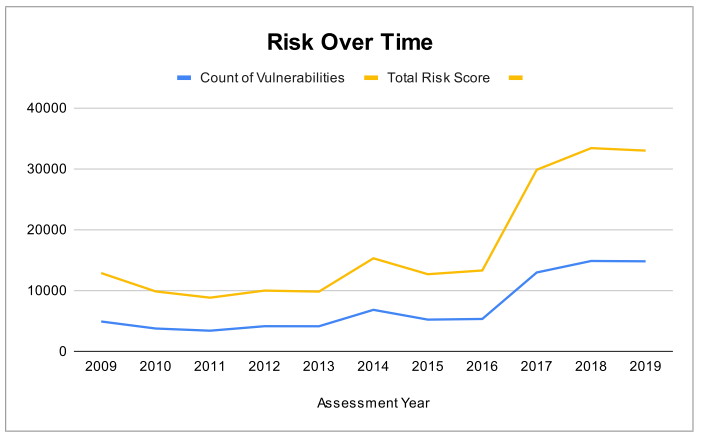
Insights:

Majority of vulnerabilities are older than 30+ days.
=> Confirms backlog; focus should be kept on clearing these before remediating other especially critical ones.



5. Trend Analysis - Risk over Time and Forecast

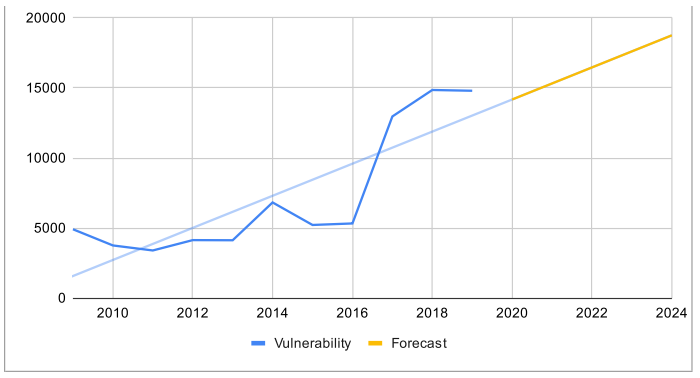
assessment_year	COUNTA of cve_id	SUM of risk_weight
2009	4909	12869
2010	3755	9854
2011	3396	8823
2012	4135	9986
2013	4125	9821
2014	6825	15295
2015	5217	12680
2016	5325	13293
2017	12965	29842
2018	14855	33402
2019	14800	32993
Grand Total	**80307**	**188858**



Filter Used	Exposure_status=detected	
assessment_year	**COUNTA of cve_id**	**Forecast**

Vulnerability Forecast

2009	4909	
2010	3755	
2011	3396	
2012	4135	
2013	4125	
2014	6825	
2015	5217	
2016	5325	
2017	12965	
2018	14855	
2019	14800	
2020		14175
2021		15321
2022		16467
2023		17613
2024		18758



Insights:

Vulnerabilities have increased constantly over the years due to increased code complexity, new ATTs and improved detection tools.
=> This data should be used for better strategies and planning for the future.

6. Remediation Priority View

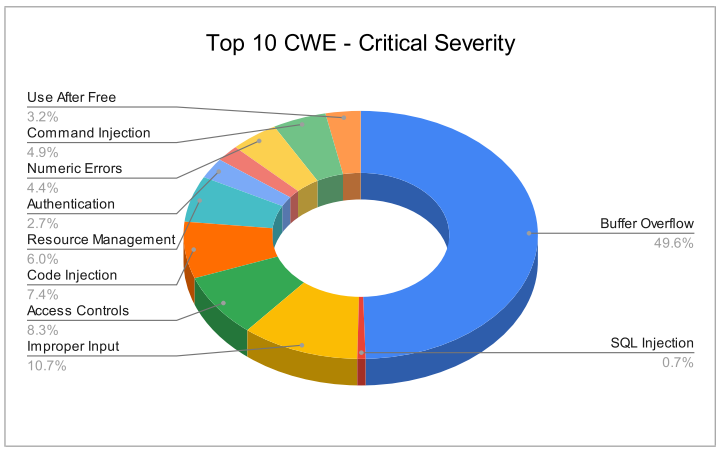
Filter Used	**Exposure_status=detected**
priority	COUNTA of cve_id
P1	11060
P2	16609
P3	48900
P4	7325
Grand Total	**83894**

Insights:

Volume is high for P3 but efforts should be risk driven not volume driven.
=> Focus on P1 and P2 more rather than get distracted by P3 to show volume in remediation.

7. Top 10 CWE

Filter Used	**Exposure_status=detected**			
cwe_name	**short_label**	**Critical**	**High**	**Total**
Improper Restriction of	Buffer Overflow	4448	2733	7181
Improper Neutralizatio	SQL Injection	67	4023	4090
Improper Input Validati	Improper Input Validatio	964	1441	2405
Permissions Privileges	Access Controls	742	1364	2106
Improper Control of Ge	Code Injection	663	754	1417
Resource Managemen	Resource Management	539	764	1303
Improper Authenticatio	Authentication	238	559	797
Improper Limitation of	Path Traversal	192	507	699
Numeric Errors	Numeric Errors	394	253	647
Improper Neutralizatio	Command Injection	441	181	622
Use After Free	Use After Free	287	288	575



Insights:

Dominance of Buffer overflow, SQL injection, improper input validation and lack of strong access controls is seen across both critical and high severities.
=> Focus efforts the development teams more on avoiding these vulnerabilities

Buffer overflow contributes to ~50% of critical vulnerabilities.
=> Team needs to practise secure coding, follow config standards and keeping the systems patched and updated.