PHOENIX
SECURITY

VULNERABILITY EXECUTIVE REPORT

Comprehensive Security Assessment

Generated on August 26, 2025

Phoenix Security Configuration System

EXECUTIVE SUMMARY

This comprehensive vulnerability assessment reveals critical security insights across your infrastructure. Our analysis covers **500 vulnerabilities** affecting **14,946 assets** with a total of **28,519 findings**. **Current Security Posture:** The analysis indicates a HIGH RISK environment with 16 critical vulnerabilities requiring immediate attention and 154 high-risk vulnerabilities needing urgent remediation.

Key Metrics

Total Vulnerabilities	500
Critical Vulnerabilities	16
High Risk Vulnerabilities	154
Assets Affected	14,946
Total Findings	28,519
Average Risk Score	583.9
Remediation Rate	0.0%

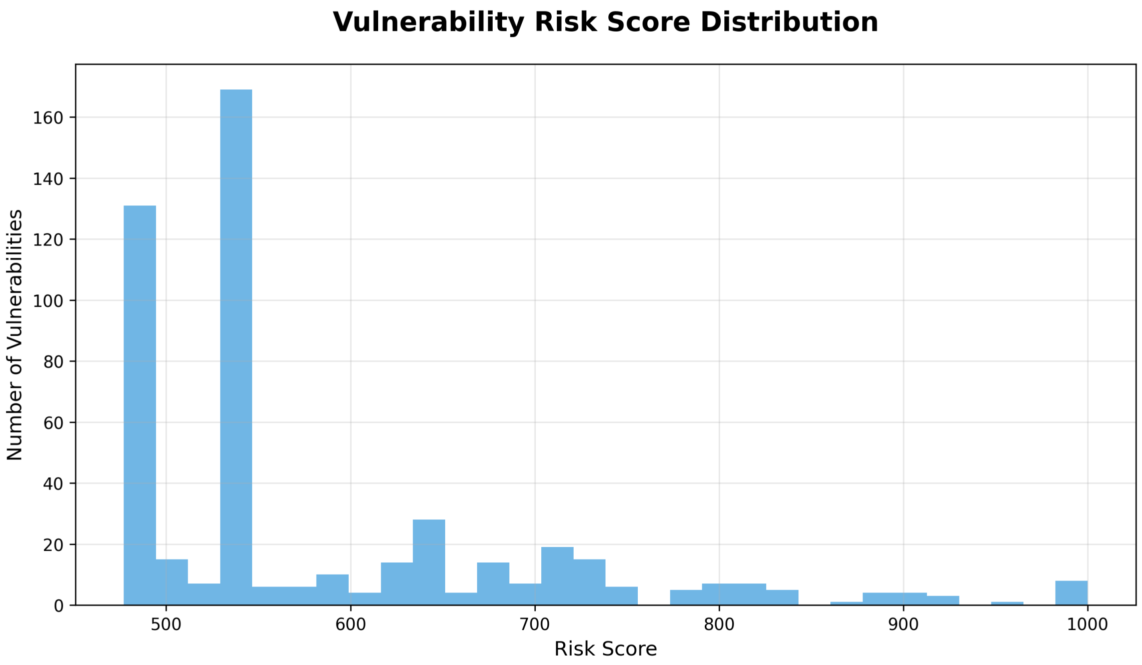
■■ CRITICAL SECURITY ALERT

IMMEDIATE ACTION REQUIRED: Your environment contains 16 critical vulnerabilities with a 0% remediation rate. The presence of known ransomware-related CVEs poses significant risk to organizational security and business continuity.

VULNERABILITY ANALYTICS & VISUALIZATIONS

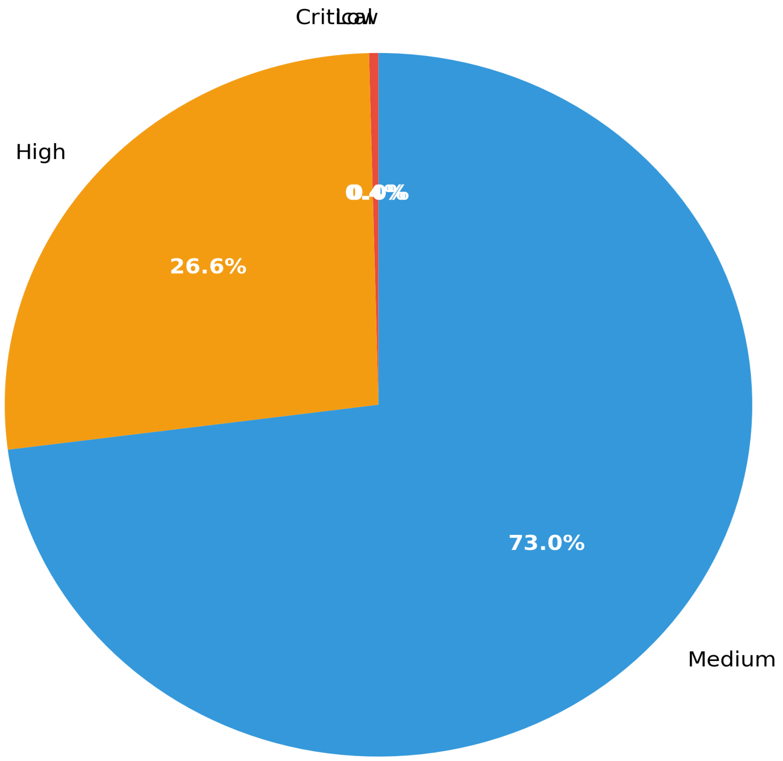
The following visualizations provide comprehensive insights into the vulnerability landscape, risk distribution, and trend analysis across your infrastructure.

1. Risk Distribution

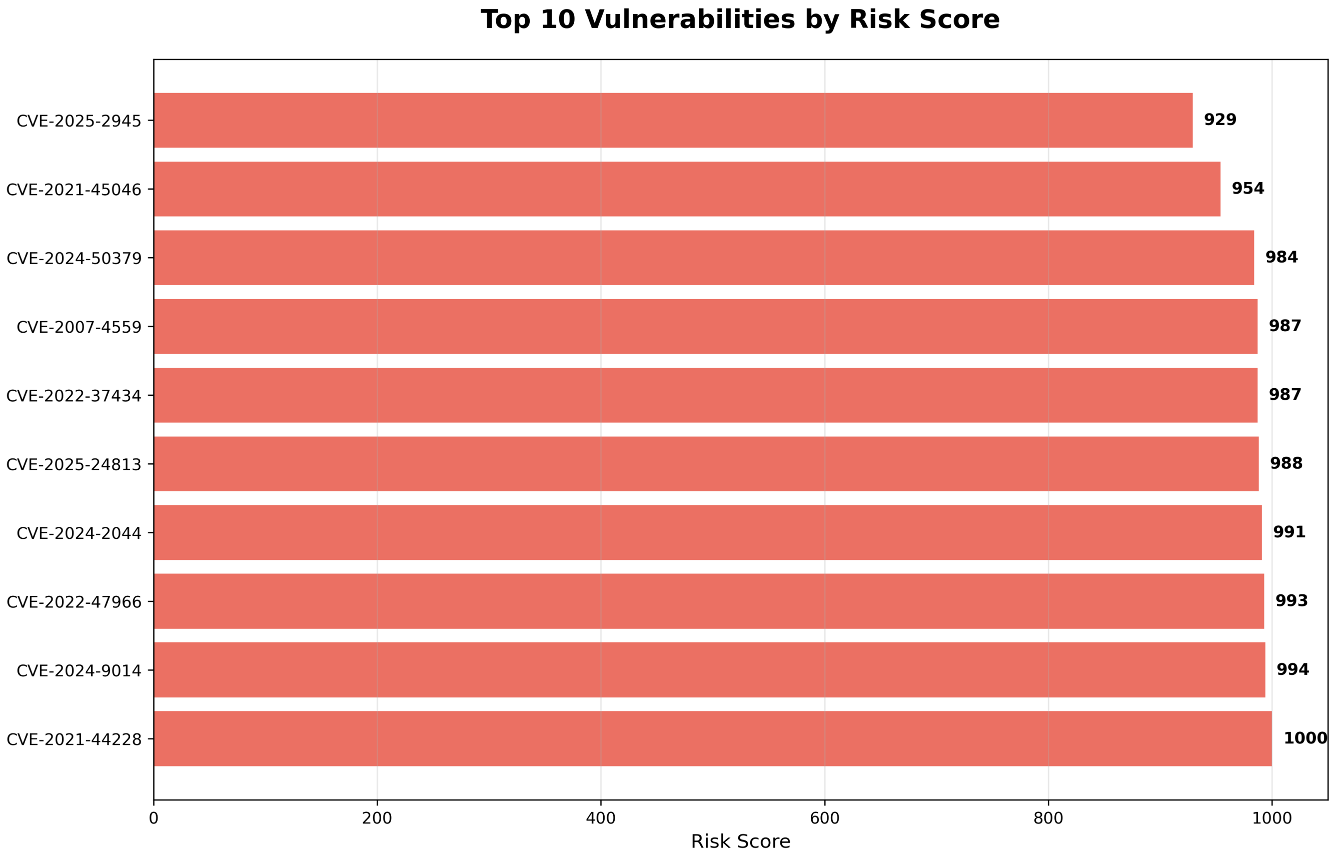


2. Severity Distribution

Vulnerability Severity Distribution

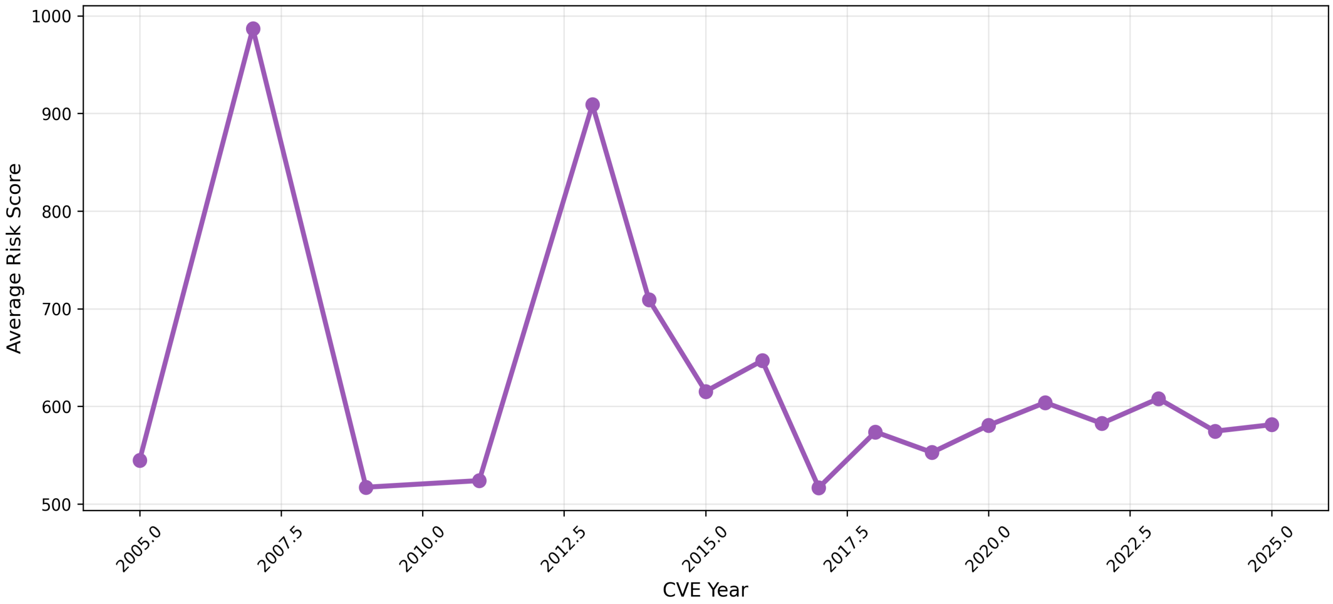


3. Top Vulnerabilities

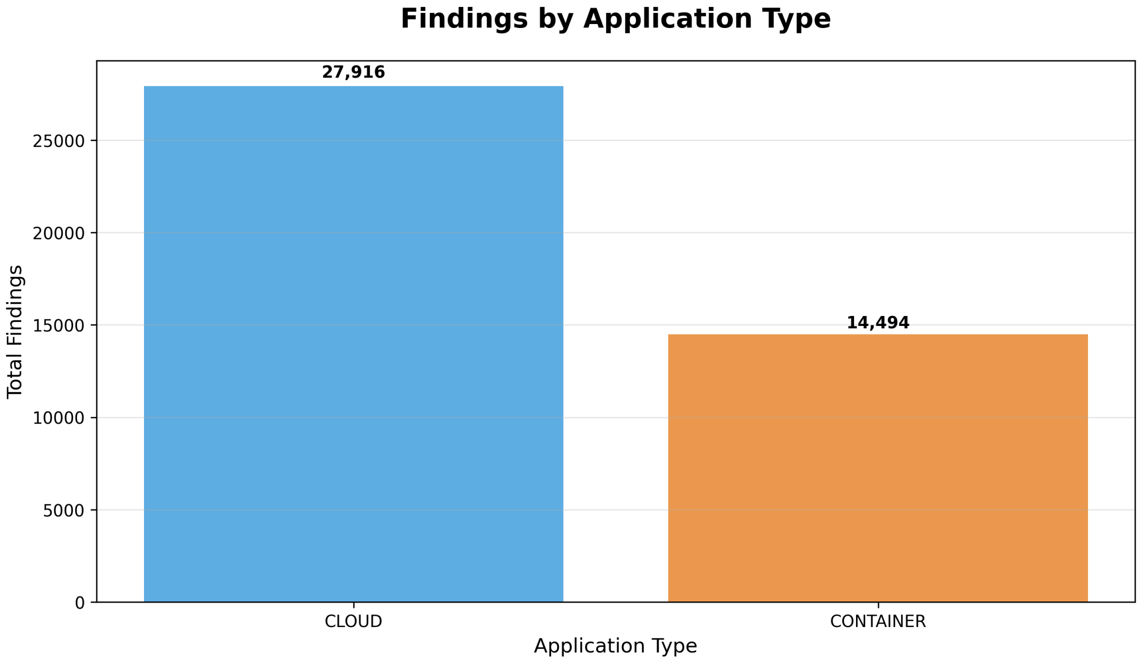


4. Year Trends

Average Risk Score by CVE Year



5. Application Trends



TOP CRITICAL VULNERABILITIES

Highest Risk Vulnerabilities Requiring Immediate Attention

CVE ID	Risk Score	Findings	Assets
CVE-2021-44228	1000	5	4
CVE-2024-9014	994	1	1
CVE-2022-47966	993	1	1
CVE-2024-2044	991	1	1
CVE-2025-24813	988	1	1
CVE-2022-37434	987	15	8
CVE-2007-4559	987	19	5
CVE-2024-50379	984	1	1
CVE-2021-45046	954	6	4
CVE-2025-2945	929	1	1

RANSOMWARE & HIGH-IMPACT THREATS

■ CRITICAL SECURITY ALERT: The following vulnerabilities are commonly exploited in ransomware attacks and advanced persistent threats (APTs). These represent the highest priority for immediate remediation.

Known Ransomware-Related CVEs Detected:

CVE ID	Risk Score	Findings	Assets
CVE-2021-44228	1000	5	4
CVE-2022-37434	987	15	8
CVE-2007-4559	987	19	5
CVE-2021-45046	954	6	4
CVE-2023-4863	918	28	8
CVE-2021-4034	841	2	1

CVE-2022-0847	833	1	1
CVE-2020-1147	829	640	2
CVE-2023-4911	821	17	5

High-Risk Exploitable Vulnerabilities:

CVE ID	Risk Score	Findings	Assets
CVE-2021-44228	1000	5	4
CVE-2024-9014	994	1	1
CVE-2022-47966	993	1	1
CVE-2024-2044	991	1	1
CVE-2025-24813	988	1	1
CVE-2022-37434	987	15	8
CVE-2007-4559	987	19	5
CVE-2024-50379	984	1	1
CVE-2021-45046	954	6	4
CVE-2025-2945	929	1	1

APPLICATION & INFRASTRUCTURE TRENDS

Analysis of vulnerability distribution across different application types and infrastructure components reveals key areas of security concern and resource allocation priorities.

Application Type	Avg Risk	Findings	Assets	Critical
CLOUD	588.2	27916	14752	115
CONTAINER	567.0	14494	5425	52

STRATEGIC RECOMMENDATIONS

■ Immediate Actions (Next 7 Days)

Critical Priority: • Address CVE-2021-44228 (Log4j) immediately - CRITICAL RANSOMWARE THREAT • Patch all vulnerabilities with risk scores ≥ 900 • Isolate assets with multiple critical vulnerabilities • Implement 24/7 monitoring for ransomware indicators • Activate incident response team for critical vulnerabilities

■ Short-term Actions (Next 30 Days)

Operational Priorities: • Develop comprehensive remediation timeline for all high-severity vulnerabilities • Strengthen security controls in CLOUD and CONTAINER environments • Increase vulnerability scanning frequency for critical assets • Update incident response procedures for identified threat vectors • Implement automated patch management where possible

■■ Long-term Strategy (Next 90 Days)

Strategic Initiatives: • Implement DevSecOps practices and shift-left security • Deploy automated vulnerability management and orchestration tools • Conduct organization-wide security awareness training • Align security practices with industry frameworks and compliance standards • Establish continuous security monitoring and threat intelligence programs

REPORT METHODOLOGY & DATA SOURCES

Data Source	WIZ Security Platform
Analysis Period	Current snapshot as of 2025-08-26
Total Vulnerabilities Analyzed	500
Risk Scoring Method	CVSS v3.1 + Environmental factors
Coverage Areas	Cloud Infrastructure, Container Security, Application Security
Report Generated By	Phoenix Security Configuration System

CONCLUSION

This vulnerability assessment reveals a **HIGH RISK** security environment requiring immediate executive attention and resource allocation. With 16 critical vulnerabilities and a 0% remediation rate, the organization faces significant exposure to ransomware attacks and advanced persistent threats. **Key Priorities:** 1. Emergency response to Log4j vulnerabilities (CVE-2021-44228) 2. Comprehensive remediation program for 154 high-risk vulnerabilities 3. Enhanced monitoring and incident response capabilities 4. Long-term security program maturation Regular monitoring and assessment are recommended to track remediation progress and identify emerging threats in this dynamic security landscape.