Harmonia Incident Response

Threat Intelligence Report - Comprehensive

Executive Summary

This report provides a comprehensive analysis of threat intelligence data collected over the past 30 days. The analysis covers 29 threat indicators from multiple sources including MITRE ATT&CK; and CISA KEV catalog.

Key Metrics

Metric	***Value***
Total Indicators	29
Average Severity	6.97
High Severity Indicators	19
Most Common Type	CVE Vulnerability
Most Active Source	CISA KEV Catalog

Threat Analysis

Threat Analysis Summary: Total Indicators Analyzed: 29 Average Severity Score: 6.97/10 High Severity Threats (≥7): 19 (65.5%) Most Common Threat Type: CVE Vulnerability (19 instances) Key Findings: • 19 high-severity threats require immediate attention • Average threat severity of 6.97 indicates moderate overall risk • CVE Vulnerability threats are the most prevalent, suggesting focused defense needed Recommendations: • Prioritize response to high-severity threats • Implement specific defenses against CVE Vulnerability threats • Consider threat hunting for related indicators • Review and update security controls based on threat patterns

Top Threats by Severity

Name	***Type***	***Severity***	***Source***

FortiOS	CVE Vulnerability	8.0	CISA KEV Catalog
DIR-859 Router	CVE Vulnerability	8.0	CISA KEV Catalog
MegaRAC SPx	CVE Vulnerability	8.0	CISA KEV Catalog
Kernel	CVE Vulnerability	8.0	CISA KEV Catalog
Multiple Routers	CVE Vulnerability	8.0	CISA KEV Catalog
Multiple Products	CVE Vulnerability	8.0	CISA KEV Catalog
Windows	CVE Vulnerability	8.0	CISA KEV Catalog
Wazuh Server	CVE Vulnerability	8.0	CISA KEV Catalog
Webmail	CVE Vulnerability	8.0	CISA KEV Catalog
Erlang/OTP	CVE Vulnerability	8.0	CISA KEV Catalog

Recommendations

Security Recommendations: 1. Immediate Actions: • Review and respond to all high-severity threats • Update threat detection rules based on observed patterns • Conduct threat hunting for related indicators 2. Strategic Improvements: • Enhance monitoring for most common threat types • Implement additional security controls where gaps exist • Develop incident response playbooks for observed threats 3. Long-term Planning: • Regular threat intelligence updates and analysis • Continuous improvement of security posture • Staff training on emerging threats and response procedures