SentinelIT Risk Intelligence Report - Powered by Diakris Zulu Cyberdefense

Generated On: 2025-06-04 10:55:22

Patch Analysis

- Apache Struts v2.3.15 is VULNERABLE (CVE: CVE-2017-5638) - Patch to: 2.3.32

- OpenSSL v1.0.2 is VULNERABLE (CVE: CVE-2016-2107) - Patch to: 1.1.1

- Tomcat v7.0.79 is VULNERABLE (CVE: CVE-2017-5647) - Patch to: 8.5.14

- Ivanti EPMM v11.4 is VULNERABLE (CVE: CVE-2025-4427) - Patch to: 11.5

Compliance Assessment

ISO 27001: NON-COMPLIANT (Issues: threatdna, risk, xsswatch)

NIST 800-53: NON-COMPLIANT (Issues: risk, dnswatch)

GDPR: NON-COMPLIANT (Issues: xsswatch, dnswatch)

HIPAA: NON-COMPLIANT (Issues: risk, dnswatch)

PCI DSS: NON-COMPLIANT (Issues: xsswatch, threatdna)

COBIT: NON-COMPLIANT (Issues: risk, threatdna, dnswatch)

Security Alerts

- [2025-06-04 10:41:27] ?? Suspicious domain keyword: login-verify-update.com contains login-verify

- [2025-06-04 10:41:27] ? Malicious IP detected: 185.100.87.202 from login-verify-update.com

- [2025-06-04 10:41:27] ?? Suspicious domain keyword: secure-pay.io contains secure-pay

- [2025-06-04 10:41:27] ? Malicious IP detected: 172.105.15.59 from secure-pay.io

- [2025-06-04 10:41:27] ? Malicious IP detected: 45.83.64.1 from cdn-update.com

- [2025-06-04 10:41:27] ? Recon/Crawler trap: cdn-update.com resolved to 45.83.64.1

- [2025-06-04 10:41:27] ? Malicious IP detected: 3.121.56.55 from bank.com

Recommendations

- Immediately patch all high-risk outdated software.
- Investigate alert sources for potential compromise.
- Enforce stricter policies for modules marked NON-COMPLIANT.
- Run SentinelIT on a scheduled basis with alert forwarding enabled.