TERRIER CVE ANALYSIS MINI REPORT

1/7/2024

QVLX LLC

600 BOULEVARD SOUTH SOUTHWEST SUITE 104, HUNTSVILLE, AL, USA
SEE COMPANION DASHBOARD: RESEARCH - QVLX LABS

NOTICE

THE RAW DATA THAT WENT INTO THIS REPORT SOURCED FROM THE MITRE CVE DATABASE. ALL CREDIT AND RESPONSIBILITY REGARDING THAT DATA BELONGS TO MITRE CORPORATION.

THE ANALYSIS PERFORMED ON THE DATA IS A PROPRIETARY COCKTAIL PROVIDED BY QVLX LLC'S TERRIER ANALYSIS PLATFORM WHICH INCLUDES A BLEND OF IN-HOUSE MACHINE LEARNING (ENSEMBLE) ALGORITHMS, OPENAI CHATGPT4, AND GOOGLE BARD ANALYSIS. ALL CREDIT PERTAINING TO USE OF CHATGPT AND BARD BELONG TO THEIR RESPECTIVE OWNERS. IN THE NAME OF ACADEMIC PROGRESS, HUMBLY THANK YOU ALL FOR THE TOOLS TO THRIVE.

KEYWORD SEARCHES YIELDING NO ENTRIES AT ALL WERE OMITTED DURING PREPROCESSING.

TERRIER CVE ANALYSIS MINI REPORT

MULTI-DIMENSIONAL AI-BASED STUDY

TABLE OF CONTENTS

CVE TREND ANALYSIS: 2018-2023

EXECUTIVE SUMMARY

This report presents an in-depth analysis of Common Vulnerabilities and Exposures (CVE) data from 2018 to 2023. It highlights key trends, vulnerabilities in various technologies, and shifts in the cybersecurity landscape. The report aims to guide cybersecurity researchers and practitioners in understanding emerging threats and formulating effective strategies to mitigate these risks.

The provided CVE data reveals concerning trends in cyber vulnerability landscape. From 2018 to 2023, we observe a significant rise in total vulnerabilities, with concerningly high percentages in common software like PHP, Java, and Javascript. Network-related vulnerabilities like CSRF and SQL injection remain prevalent, while buffer overflow and kernel exploits persist despite known mitigation strategies. Open-source software vulnerabilities are on the rise, while classified CVEs have noticeably increased, potentially indicating more sophisticated threats.

DETAILED TREND ANALYSIS

CROSS-SITE VULNERABILITIES

- **Rising Trend**: Consistent increase, especially in 2022 and 2023.
- **Implications**: Weaknesses in input validation and session management.

PROGRAMMING LANGUAGE-SPECIFIC VULNERABILITIES

- **PHP, Java, Python**: Fluctuating vulnerabilities; evolving attack vectors.
- **Emergence of Rust**: Growing interest necessitates research in secure coding at the system level.

MOBILE AND IOT SECURITY

- **IoT**: Increased vulnerabilities in 2021; need for robust security protocols.
- **Mobile Platforms (iOS, Android)**: Ongoing challenges in OS and application security.

BUFFER OVERFLOW VULNERABILITIES

- **Persistent Threat**: High rates continue, emphasizing the need for better memory management.

SQL INJECTION VULNERABILITIES

- **Rising Concern**: Growth, particularly in 2022, indicates ongoing database security issues.

CLASSIFIED AND SENSITIVE DATA VULNERABILITIES

- **Sensitive Data**: Focus on data protection mechanisms and encryption is necessary.

SOFTWARE VULNERABILITIES

- **Leading Languages**: PHP, Java, and Javascript vulnerabilities necessitate security best practices.

NETWORK VULNERABILITIES

- **Persistent Threats**: Common issues like CSRF, Cross-site, and SQL injection remain prevalent.

KERNEL AND ESCALATION RISKS

- **Significant Risks**: Vulnerabilities in kernel and privilege escalation demand attention.

OPEN-SOURCE CONCERNS

- **Rising Vulnerabilities**: Increased scrutiny and community mitigation efforts are needed.

YEARLY OBSERVATIONS AND IMPLICATIONS

- **2018-2019**: Balance across platforms; shift towards mobile and web applications.
- **2020**: Significant overall increase; emergence of Rust; spike in CVEs.
- **2021**: Peak in Java and IoT vulnerabilities; open-source software concerns.
- **2022**: PHP and SQL vulnerabilities peak; rise in classified CVEs.
- **2023**: Increase in cross-site vulnerabilities; continued growth in overall vulnerabilities.

STRATEGIC RECOMMENDATIONS

1. **Advanced Web Security Research**: Focus on input validation, session management, and CSRF/XSS defenses.
2. **Holistic Approach to Legacy and Emerging Technologies**: Address both traditional and modern technology challenges.
3. **Secure Coding and Frameworks**: Emphasize secure practices in PHP, Java, Python, and languages like Rust.
4. **Mobile and IoT Security Enhancements**: Develop robust protocols for mobile platforms and IoT devices.
5. **Enhanced Network Protection**: Prioritize network security, including VPN enhancements and DoS attack mitigation.
6. **Database Security Innovations**: Implement new SQL injection prevention methods.
7. **Data Protection Mechanisms**: Strengthen encryption and data protection.
8. **Memory Protection and Code Hardening**: Mitigate buffer overflow vulnerabilities.
9. **Prompt Patching**: Address kernel and privilege escalation vulnerabilities swiftly.
10. **Open-Source Software Community**: Promote security best practices and proactive measures.

11. **IoT Device Monitoring**: Ensure secure development practices for connected devices.
12. **Classified CVE Response**: Collaborate with security agencies for sophisticated threat handling.
13. **Security Awareness Training**: Foster a proactive security culture.
14. **Continuous Vulnerability Assessment**: Regularly assess and address potential vulnerabilities.

CONCLUSION

Focus on input validation, session management, and CSRF/XSS defenses.
By implementing these strategic recommendations and staying informed about evolving cyber threats, organizations can significantly reduce their risk of cyberattacks and strengthen their overall security posture.

DIMENSIONS ANALYZED AND CLUSTERING

Dimension	Cluster
open source	Access
proprietary	Access
OpenSource	Access
Open-Source	Access
patented	Access
Commercial	Access
CUI	Access
classified	Access
unclassified	Access
PII	Access
sensitive	Access
non-sensitive	Access
android	Device
xbox	Device
playstation	Device
nintendo	Device

Dimension	Cluster
traffic	Experimental
IoT	Experimental
Ransomware	Exploitation
VPN	Exploitation
Mitm	Exploitation
Denial-of-Service	Exploitation
CSRF	Exploitation
IDOR	Exploitation
Clickjack	Exploitation
SSRF	Exploitation
Heap Overflow	Exploitation
Buffer Overflow	Exploitation
Side-Channel	Exploitation
Replay	Exploitation
Secure boot	Exploitation
Phishing	Exploitation
Brute force	Exploitation
Hypervisor	Exploitation
Kernel	Exploitation
Escalation	Exploitation
Database	Exploitation
Cross-site	Exploitation
Network	Exploitation

Dimension	Cluster
SQL	Exploitation
x86	Hardware
amd	Hardware
x64	Hardware
intel	Hardware
arm32	Hardware
arm64	Hardware
arm	Hardware
powerpc	Hardware
mips	Hardware
riscv	Hardware
sparc	Hardware
avr	Hardware
Java	Language
C++	Language
PHP	Language
Javascript	Language
swift	Language
Rust	Language
Nim	Language
nim	Language
Python	Language
rust	Language

Dimension	Cluster
LynxOS	OS
windows	OS
macos	OS
linux	OS
iOS	OS
QNX	OS
VxWorks	OS
Zephyr	OS