TERRIER CVE ANALYSIS MINI REPORT

AI/ML Focused Edition 1/8/2024

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 (AI/ML FOCUS)

MULTI-DIMENSIONAL AI-BASED STUDY

TABLE OF CONTENTS

CVE DATA ANALYSIS REPORT: AI AND ML VULNERABILITIES (2018-2023)

EXECUTIVE SUMMARY

- A noticeable increase in AI/ML-related CVEs in recent years, with a significant surge in 2021 and 2022.
- AI/ML vulnerabilities, particularly in Machine Learning, represent a growing but still small proportion of total CVEs.
- Consistent presence of vulnerabilities related to Clustering, PCA, Regression, Robots, and new emergence of GPT, chatGPT, and supervised learning techniques.

DETAILED TREND ANALYSIS

- **Machine Learning Surge**: A sharp rise in ML-related CVEs observed in 2021-2022.
- **Overall AI/ML CVEs**: Growing numbers of AI/ML CVEs indicate emerging risks in these technologies.
- **Consistent Vulnerabilities**: Persistent CVEs across years in Clustering, PCA, Regression, and Robot-related areas.
- **Emergent Techniques**: New vulnerabilities involving techniques like GPT, chatGPT, and supervised learning were noted in 2023, highlighting evolving threats.

YEARLY OBSERVATIONS AND IMPLICATIONS

- **2018-2020**: Initial phase with low AI/ML CVEs, PCA and Robot-related vulnerabilities more noticeable. PCA and other acronyms that have multiple meanings could be inaccurate in this study as word of caution.
- **2021**: Marked increase in ML-related CVEs, indicating a pivot towards ML security concerns.
- **2022**: Continued growth in ML CVEs; stable occurrence of other AI/ML vulnerabilities.
- **2023**: Introduction of CVEs in specific AI/ML techniques, showing potential vulnerabilities in newer AI/ML methods.

STRATEGIC RECOMMENDATIONS

1. **Prioritize ML Security Research**: Allocate resources to investigate ML algorithm vulnerabilities.
2. **Monitor AI/ML CVE Trends**: Track CVEs to identify emerging threats and direct mitigation efforts.
3. **Focus on Consistent Vulnerabilities**: Proactively address known vulnerabilities in Clustering, PCA, Regression, and Robotics.
4. **Research Emerging Techniques**: Investigate vulnerabilities in emerging AI/ML techniques such as GPT, chatGPT, and supervised learning.

5. **Incorporate AI/ML Security in Development**: Integrate security measures in the development and deployment of AI/ML systems.
6. **Promote Responsible AI/ML Development**: Advocate for ethical, secure development practices within the AI/ML community.
7. **Continuously Adapt and Update Security Measures**: Ensure AI/ML security practices are dynamic and evolve with technological advancements.

CONCLUSION

The growth in AI/ML-related CVEs highlights the increasing importance of securing these technologies. Cybersecurity strategies must evolve in parallel with technological advancements in AI and ML. Continuous vigilance, research, and adaptation are key to mitigating emerging threats in this rapidly advancing field.

DIMENSIONS ANALYZED AND CLUSTERING

Dimension	Cluster
Machine learning	AI/ML
Artificial intelligence	Access
chatgpt	Access
gpt	Access
supervised	Access
Recommender	Access
Predictor	Access
Classifier	Access
Clustering	Access
PCA	Access
SVD	Access
Eigen	Access
Bayes	Device
Regression	Device
forecasting	Device

Dimension	Cluster
natural language	Device
deep learning	Experimental
ensemble	Experimental
neural network	Exploitation
autonomous	Exploitation
computer vision	Exploitation
robot	Exploitation
watson	Exploitation
swarm	Exploitation