Vulnerability Management

SEKURENET

EPSS vs. CVSS: The Best Approach to Prioritize Vulnerabilities

The CVSS is an industry-standard framework for quantifying the severity of vulnerabilities. It uses a scoring system (0.0–10.0) based on metrics such as exploitability, impact, and environmental factors. While CVSS offers a clear structure for assessing vulnerabilities, its static nature can lead to inefficiencies.

- Pros: Widely adopted, offering a standardized way to rank vulnerabilities.
- Cons: Doesn't account for real-time threat intelligence, leading to an inflated sense of urgency for low-priority vulnerabilities.

EPSS, a relatively new framework, predicts the likelihood of a vulnerability being exploited within a set timeframe. It combines CVSS base metrics with real-world data, such as exploitation trends observed in the wild.

- Pros: Data-driven, making it dynamic and context-aware.
- Cons: Limited adoption and requires access to current exploitation data.

What's Better?

The choice between EPSS and CVSS depends on your organization's goals:

- For Critical Environments: Use EPSS to focus on actively exploited vulnerabilities.
- For Compliance: CVSS may be better suited due to its standardized scoring and regulatory recognition.

Exploitable Machine Learning Vulnerabilities

The Growing Risks in ML Ecosystems

Machine learning (ML) models are increasingly integral to software systems, but they come with unique vulnerabilities.

Adversarial Attacks: Small, imperceptible changes
in input data that cause ML models to misbehave (e.g., fooling image recognition systems).

Data Poisoning: Injecting malicious data into training datasets to manipulate model outputs.

Model Stealing: Extracting a proprietary ML model's architecture and weights using query access.

Mitigation Strategies

- **Input Validation**: Apply robust preprocessing to detect adversarial patterns.
- **Secure Training Pipelines**: Use trusted datasets and monitor for anomalies during training.
- **Regular Model Audits**: Continuously test models for robustness against adversarial inputs.