

Beyond CVSS: Context-Aware Exploitability Assessment of Vulnerabilities in HPC Containers

Motivation & problems

- HPC container Images contains thousands of vulnerabilities
- Security tools rely on CVSS and EPSS
- However, these metrics do not consider context-specific constraints
- Many vulnerabilities are not reachable or triggerable in practice

Severity ≠ Real-world risk

Approach & Contributions

Research Question:

- Are Vulnerabilities in HPC containers actually exploitable under realistic HPC conditions?

Key Idea:

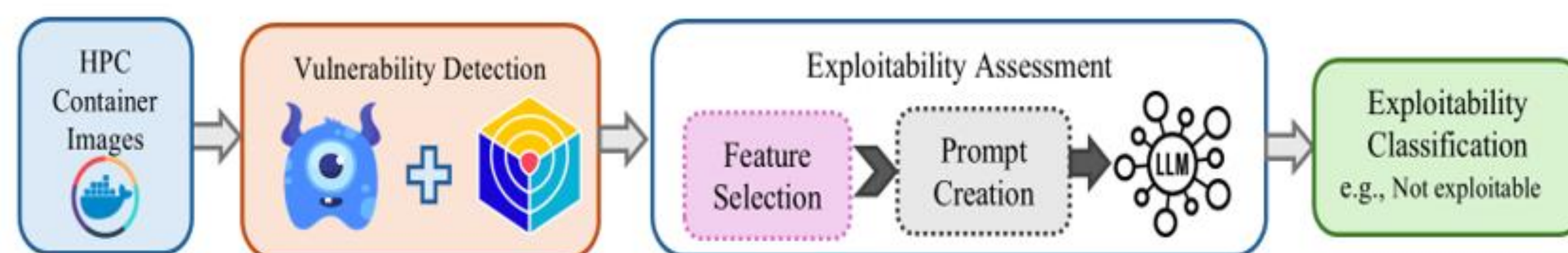
- Exploitability is context-dependent, not severity-based

Contribution:

- Context-aware exploitability assessment framework
- Structured prompt-based LLM reasoning pipeline
- Large-scale evaluation (**100** container images, **~170k** CVEs)

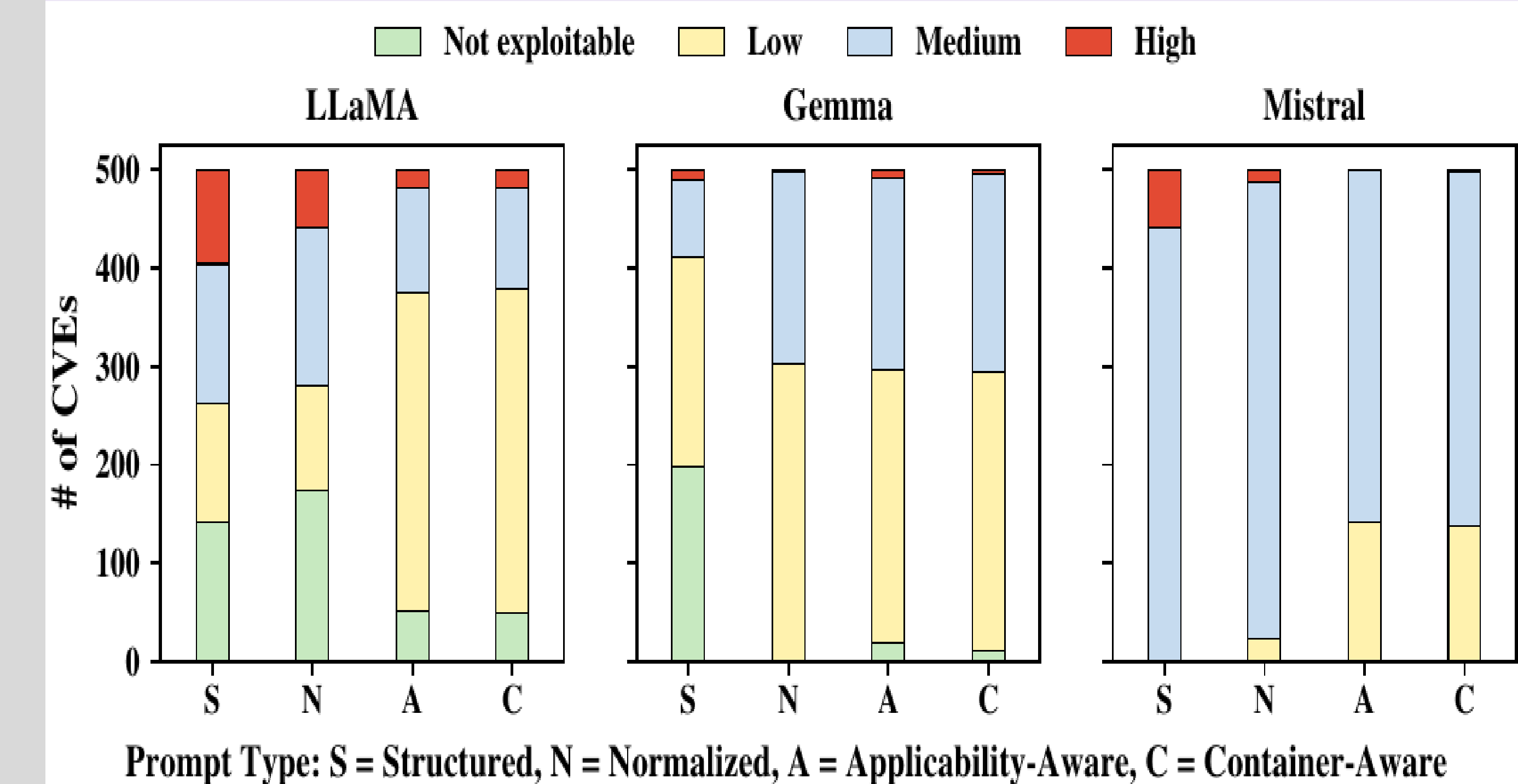
Methodology

- **100** HPC container images (**~170K CVEs**) were used as the dataset.
- Three open-weight LLMs were evaluated via vLLM on multi-NVIDIA L40s GPUs.
- Each CVE was assessed across **5 independent inference runs** with majority-vote consensus.
- Four prompt tiers were tested: Structured, Normalized, Applicability-Aware, and Container-Aware.
- Exploitability was classified into **four tiers**: High, Medium, Low, and Not Exploitable.



Findings

- Container-aware prompting significantly reduces High risk classifications from **11.0% to 1.7% across all models**, with up to 75.8% of vulnerabilities classified as low risk.
- Mistral achieves the highest consensus at 99.9% followed by **Gemma at 93.3% and LLaMa at 69.7%** with no extreme cross model disagreements observed.



Conclusions & Impact

- Container aware prompting cuts severe exploitability overestimation (upto 99.9% consensus) across all three LLMs
- Package presence, remediation status, and runtime constraints are the key signals driving exploitability reasoning.
- Context is not optional: generic prompting fails HPC vulnerability prioritization.

References

- E. Oseghale, Y. Cheng, S. Li, D. Zhang, S.-H. Lim, Z. Cao, X. Gao, and Y. Ji, "Container image security in hpc: A comprehensive large-scale evaluation," in 2025 IEEE Cloud Summit. IEEE, 2025, pp. 54–59