Trend Micro Warns of Thousands of Exposed AI Servers

Latest research reveals mounting infrastructure-level risks from diverse components

DALLAS, July 29, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today urged AI engineers and IT leaders to heed best practices in developing and deploying secure systems, or risk exposure to data theft, poisoning, ransom, and other attacks.

To learn more about how network defenders and adversaries are using AI, read*Trend Micro State of AI Security Report, 1H 2025: https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-micro-state-of-ai-security-report-1h-2025*

Rachel Jin, Chief Enterprise Platform Officer at Trend: "AI may represent the opportunity of the century for global businesses. But those rushing in too fast without taking adequate security precautions may end up causing more harm than good. As our report reveals, too much AI infrastructure is already being built from unsecured and/or unpatched components, creating an open door for threat actors."

Trend's report highlights several AI-related security challenges:

1) **Vulnerabilities/exploits in critical components**

Organizations wishing to develop, deploy and use AI applications must leverage multiple specialized software components and frameworks, which may contain vulnerabilities one may find in regular software. The report reveals zero-day vulnerabilities and exploits in core components including ChromaDB, Redis, NVIDIA Triton, and NVIDIA Container Toolkit.

2) **Accidental exposure to the internet**

Vulnerabilities are often the result of rushed development and deployment timelines, as are instances whenAI systems are accidentally exposed to the internet, where they can be probed by adversaries. As detailed in the report, Trend has found 200+ ChromaDB servers, 2,000 Redis servers, and 10,000+ Ollama servers exposed to the internet with no authentication.

3) **Vulnerabilities in open-source components**

Many AI frameworks and platforms use open-source software libraries to provide common functionality. However, open-source components often contain vulnerabilities that end up creeping into production systems, where they are hard to detect. At the recent Pwn2Own Berlin, which featured a new AI category, researchers uncovered an exploit for the Redis vector database, which stemmed from an outdated Lua component.

4) **Container-based weaknesses**

A great deal of AI infrastructure runs on containers, meaning it is exposed to the same security vulnerabilities and threats that impact cloud and container environments. As outlined in the report, Pwn2Own researchers were able to uncover an exploit for the NVIDIA Container Toolkit. Organizations should sanitize inputs and monitor runtime behavior to mitigate such risks.

Stuart MacLellan, CTO, NHS SLAM: "There are still lots of questions around AI models and how they could and should be used. We now get much more information now than we ever did about the visibility of devices and what applications are being used. It's interesting to collate that data and get dynamic, risk-based alerts on people and what they're doing depending on policies and processes. That's going to really empower the decisions that are made organizationally around certain products."

Both the developer community and its customers must better balance security with time to market in order to mitigate the risks outlined above. Concrete steps could include:

- Improved patch management and vulnerability scans
- Maintaining an inventory of all software components, including third-party libraries and subsystems
- Container management security best practices, including using minimal base images and runtime security tools
- Configuration checks to ensure AI infrastructure components, like servers aren't exposed to the internet

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organizations to simplify and secure their connected world.

www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2025-07-29-Trend-Micro-Warns-of-Thousands-of-Exposed-AI-Servers