TrendAI™ Zero Day Initiative Leads Industry Remediation at Pwn2Own Berlin

Ethical hackers earn over $1.2 million in prizes at event sponsored by NVIDIA

DALLAS, May 18, 2026 /PRNewswire/ -- TrendAI™, the enterprise cybersecurity business fromTrend Micro Incorporated (TYO: 4704; TSE: 4704), today celebrated the efforts of the global security research community at Pwn2Own Berlin. Contestants discovered and disclosed 47 unique zero-day vulnerabilities across categories including AI databases, coding agents, web browsers, enterprise applications, servers, and more.

Rachel Jin, Head of TrendAI: "TrendAI™ uses the deepest threat intelligence in the industry to protect our customers. We use the vulnerabilities discovered at Pwn2Own to empower vendors to patch these vulnerabilities quickly, while also offering our customers protection well ahead of the rest of the industry via virtual patching. As AI tools and infrastructure continue to become central to businesses functions, staying ahead of vulnerabilities will be as critical as ever."

NVIDIA joined the event as a first-time sponsor of Pwn2Own, bringing its own category of products for researchers to target for vulnerability disclosures. Megatron Bridge, NV Container Toolkit, and Dynamo were included.

The disclosures made through the ZDI at Pwn2Own and year-round allow vendors to quickly understand and fix vulnerabilities before cybercriminals exploit them, ultimately benefiting organizations and end users of the impacted software or hardware. ZDI research has shown that vendors are increasingly neglecting to patch software vulnerabilities that are disclosed to them. Through ZDI's coordinated disclosure process, TrendAI Vision One™ customers receive are protected an average of three months ahead of the rest of the industry.

Highlights from the event included:

- Orange Tsai (@orange_8361) of DEVCORE Research Team chained 3 bugs to achieve Remote Code Execution as SYSTEM on Microsoft Exchange, earning $200,000. They also chained 4 logic bugs to achieve a sandbox escape on Microsoft Edge, earning $175,000.
- Splitline (@splitline) of DEVCORE Research Team chained 2 bugs to exploit Microsoft SharePoint, earning $100,000.
- Nguyen Hoang Thach (@hi_im_d4rkn3ss) of STARLabs SG (@starlabs_sg) used a Memory Corruption bug to exploit VMware ESXi with the Cross-tenant Code Execution add-on, earning $200,000 and 20 Master of Pwn points.
- Chompie of IBM X-Force Offensive Research (XOR) used a single bug to exploit NV Container Toolkit, earning $50,000.

A total of $1,298,250 in prizes were awarded to the participants. The next competition, Pwn2Own Cork, will be held in October.

About TrendAI™
TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. Global Fortune 500 companies rely on TrendAI™ to cut risk and stop threats up to three months earlier, powered by world-leading threat and attack intelligence. Through deep ecosystem partnerships with market leaders like NVIDIA, Anthropic, AWS, Google, and Microsoft, TrendAI™ empowers your organization to securely drive forward at the speed of AI. AI Fearlessly. Learn more at trendaisecurity.com.

SOURCE TrendAI

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

---

Additional assets available online: Video (1)