

Presseinformation

TrendAI™ Zero Day Initiative™ vergibt bei Hacking-Wettbewerb Pwn2Own Preisgelder in Höhe von über 1,2 Millionen US-Dollar

98 Zero-Day-Schwachstellen bei dreitägigem Hacking-Wettbewerb entdeckt und weitere Erkenntnisse für die schnellere Erkennung und Behebung von Schwachstellen im KI-Zeitalter gewonnen

Wallisellen und Cork, Irland, 13. Oktober 2026 – TrendAI™, weltweit führender Anbieter von KI-Sicherheit und der Enterprise-Cybersecurity-Geschäftsbereich von Trend Micro Incorporated (TYO: 4704; TSE: 4704), würdigte im Rahmen des Ethical-Hacking-Wettbewerbs Pwn2Own Ireland die Arbeit der internationalen Sicherheitsforschungs-Community mit Preisgeldern in Höhe von insgesamt 1.262.000 US-Dollar. Die Teilnehmer entdeckten und meldeten 98 bislang unbekannte Schwachstellen in verschiedenen Kategorien, darunter Mobiltelefone, Smart-Home-Geräte, Wellness-Geräte, Drucker, Messaging, KI-Infrastruktur und KI-Coding-Agenten.

Die in der vergangenen Woche beim Pwn2Own auf der Bühne gezeigten Geräte sind bewusst alltäglich: Smartphones, Drucker, Smart-Home-Geräte und Wearables. Gelingt es einem Sicherheitsforscher, mehrere Schwachstellen miteinander zu kombinieren, um die Kontrolle über ein solches Gerät zu übernehmen, wird ein Prozess sichtbar, der normalerweise im Verborgenen abläuft. Derselbe Prozess und häufig auch dieselben Arten von Schwachstellen betreffen die Systeme auf Unternehmensebene, wie beispielsweise im E-Commerce, dem Bankwesen, kritischen Infrastrukturen und dem Gesundheitswesen.

Die über die TrendAI Zero Day Initiative (ZDI) beim Pwn2Own und darüber hinaus gemeldeten Schwachstellen helfen Herstellern, Sicherheitslücken schnell zu verstehen und zu beheben, bevor Cyberkriminelle sie ausnutzen können. Davon profitieren letztlich Unternehmen und Endnutzer der betroffenen Software oder Hardware. Denn Untersuchungen von TrendAI zeigen, dass Hersteller die Behebung gemeldeter Software-Schwachstellen durch Sicherheitsupdates zunehmend vernachlässigen.

„Die Kenntnis dieser Schwachstellen trägt auch dazu bei, Kunden von TrendAI durch virtuelles Patching zu schützen“, erklärt Dustin Childs, Head of Threat Awareness bei der TrendAI Zero Day Initiative. „Der nachhaltige Nutzen einer solchen Veranstaltung liegt zudem in den Erkenntnissen, die Sicherheitsverantwortliche daraus gewinnen. Jede auf der Bühne demonstrierte Exploit-Kette vermittelt uns neues Wissen darüber, wie moderne Systeme kompromittiert werden können. Diese Informationen fließen direkt in die Weiterentwicklung unserer eigenen Forschungskompetenz ein, damit wir die

nächste Schwachstelle schneller entdecken, validieren und beheben können. Da KI-Tools und -Infrastrukturen für Geschäftsprozesse immer wichtiger werden, wird es weiterhin entscheidend sein, Schwachstellen frühzeitig zu erkennen und ihnen zuvorzukommen.“

Zu den Höhepunkten des Wettbewerbs zählten:

- **Ikotas Labs, Inc.** gewann den Titel „Master of Pwn“ und ein Preisgeld von 300.000 US-Dollar. Das Team kombinierte mehrere Schwachstellen erfolgreich miteinander, um ganz am Ende des dreitägigen Wettbewerbs das Google Pixel 10 zu kompromittieren. Ikotas Labs, Inc. ist das erste japanische Team, das den Titel „Master of Pwn“ gewonnen hat.
- **Xint**, das den zweiten Platz im Wettbewerb belegte, erhielt 150.000 US-Dollar für die erfolgreiche Demonstration eines Remote-Exploits gegen das Google Pixel 10.
- **Interrupt Labs** erhielt 5.000 US-Dollar, nachdem das Team erfolgreich die Kontrolle über den Drucker Lexmark CX532adwe übernommen und das Computerspiel DOOM auf dessen Bildschirm zum Laufen gebracht hatte.

„Die Live-Demonstrationen von Zero-Day-Exploits auf der Bühne zu verfolgen war äusserst spannend“, sagt Caroline Kiel, CEO des Professional-Services-Anbieters PingUs Solutions. „Es ist ein positives Signal, dass die Hersteller selbst vor Ort waren, um die Research-Community dazu zu ermutigen, Schwachstellen in ihren Produkten aufzudecken. Bei Pwn2Own werden neue Erkenntnisse aus der Schwachstellenforschung unmittelbar in Schutzmassnahmen umgesetzt. Das zeigt, wie konsequent sich TrendAI für die Sicherheit im gesamten IT-Ökosystem einsetzt.“

Weitere Informationen

Durch den koordinierten Offenlegungsprozess der TrendAI™ ZDI sind Nutzer der Cybersecurity-Plattform TrendAI Vision One durchschnittlich 115 Tage früher geschützt als der übrige Markt.

Der nächste Pwn2Own-Wettbewerb ist für Anfang 2027 geplant. Weitere Informationen finden Sie unter: <https://www.zerodayinitiative.com/blog>

Über TrendAI™

TrendAI™, weltweit führender Anbieter von KI-Sicherheit und der Enterprise-Geschäftsbereich von Trend Micro, ermöglicht Organisationen vollständige Transparenz und Governance ihrer KI-Nutzung sowie konsolidierte Sicherheit, die Vertrauen schafft, Innovation fördert und Risiken eliminiert. Weltweit vertrauen die grössten Unternehmen und Regierungsbehörden in 185 Ländern auf TrendAI™, um ihre gesamte Organisation zu schützen – von Identitäten über Infrastrukturen bis hin zu Daten.

Globale Fortune-500-Unternehmen verlassen sich auf TrendAI™, um Bedrohungen bis zu 115 Tage früher zu stoppen – gestützt auf führende Bedrohungs- und Angriffsanalysen. Durch enge



Partnerschaften mit führenden Anbietern wie NVIDIA, Anthropic, AWS, Google und Microsoft befähigt TrendAI™ Organisationen, sicher mit der Geschwindigkeit von KI voranzuschreiten. Diese Allianzen zeigen Ergebnisse: TrendAI™ ist der erste KI-Sicherheitsanbieter aus der Region Asien-Pazifik-Japan, der die Marke von einer Milliarde US-Dollar kumuliertem globalem Umsatz im AWS Marketplace überschritten hat.

Mit TrendAI™ erhalten Unternehmen einen klaren Überblick darüber, wie KI in ihren Umgebungen eingesetzt wird, können neu entstehende Risiken identifizieren und schneller reagieren. CISOs können damit ihre Sicherheitsarchitektur vereinfachen und Geschäftsführungen erhalten das Vertrauen, Innovationen sicher voranzutreiben.
AI Fearlessly.

Pressekontakt:

Brand Affairs AG
Mischa Keller
Mühlebachstrasse 8
8008 Zürich
Telefon: +41 (0) 79 380 95 86
E-Mail: mischa.keller@brandaffairs.ch
Internet: www.brandaffairs.ch

Unternehmenskontakt:

Trend Micro Deutschland GmbH
Tobias Grabitz
Parkring 29
D-85748 Garching b. München
Telefon: +49 (0) 170 144 23 68
E-Mail: tobias_grabitz@trendmicro.com
Internet: www.trendaisecurity.com