Trend Micro Zero Day Initiative™ Sheds Light on Software Vulnerabilities: Customers Protected up to 70 Days Before Patches

ZDI pays over $1 million to researchers in hacking contest targeting web browsers, enterprise software and more

DALLAS, April 2, 2024 /PRNewswire/ -- Global cybersecurity leaderTrend Micro Incorporated (TYO: 4704; TSE: 4704) has announced the outcomes from its Pwn2Own ethical hacking contest, hosted by the Zero Day Initiative (ZDI), which included identification of new vulnerabilities in Windows, Linux, Tesla, Chrome, VMWare, and other widely used technology. Trend customers benefit from same-day protections and the rest of the world benefits as soon as software patches are released.

One of the biggest challenges for organizations in managing cyber risk is dealing with the volume of emerging threats against available security resources. Software companies and electric vehicle (EV) manufacturers must triage and prioritize what vulnerabilities they fix, leading to an all-time high of known but unpatched problems. While the industry average time to respond and protect sits above 70 days, ZDI research enables protection for Trend customers almost immediately.

While average time to protect is over 70 days, ZDI research enables protection for Trend customers almost immediately.

Matt Guzzi, Information Systems Administrator, South Carolina State Library: "We count on developers of the software we use to patch vulnerabilities. Until that happens, we face greater exposure to cyberattacks. Trend's threat intelligence allows us to be protected from new exploits immediately."

Key highlights from Pwn2Own Vancouver 2024:

- Researchers disclosed 29 unique 0-day vulnerabilities and earned $1,132,500 in prizes
- All major web browsers were compromised during the event
- The Tesla Model 3 ECU was hacked with an over-the-air exploit
- Researchers demonstrated the first ever Docker escape (when an attacker is able to break out of a container and gain access to the host system) at Pwn2Own

Disclosures made to the ZDI by researchers at Pwn2Own and independently year-round allow software developers to learn about vulnerabilities before cybercriminals find them. While this ultimately benefits enterprises, supply chains, infrastructure, and customers, ZDI research has shown that vendors are increasingly neglecting to respond to disclosures in a timely manner.

Frank Dickson, Group Vice President for Security and Trust at IDC: "Cyber threats remain on track to continue proliferating, but software patches are lagging by comparison. This leaves organizations exposed to additional cyber risk beyond their control. Security vendors that can spot vulnerabilities early and bridge this critical gap with virtual patches will provide significant additional value to customers."

When vulnerabilities are discovered, enterprises and cybersecurity vendors simply have to wait for a patch to be released. In-depth threat awareness generated by Pwn2Own enables Trend to protect its customers with virtual patches to ensure there is no lapse in protection. This applies to over 1,000 vulnerabilities per year directly attributed to disclosure through the ZDI.

Dustin Childs, Head of Threat Awareness at the Zero Day Initiative: "While everyone is talking about security issues with hot topics like TikTok and ChatGPT, many of the most serious threats are in the backbones of major operating systems used by billions of people worldwide—many of which are left unaddressed by today's widely known big tech companies. Researchers participating in Pwn2Own do the critical work of finding these exploits before the bad guys do and sharing them with Trend and the ZDI. This is a resource that no one else has and marks a significant differentiator for Trend's threat intelligence and prevention capabilities."

Discovering and mitigating vulnerabilities in the real world has a direct correlation to reducing cyber risk across the board. Security teams at organizations of all sizes are increasingly overwhelmed by threats that exceed their purview, which can include threats to office equipment, industrial equipment, connected vehicles and EVs, and employees' home office devices such as smartphones, NAS devices, cameras, printers, routers and personal vehicles.

Pwn2Own pays bounties to researchers for the responsible discovery and disclosure of vulnerabilities in software and hardware that billions of people rely on daily. This research improves Trend's industry-leading threat intelligence and uncovers new software exploitation techniques. The contest also pushes the industry forward in the fight against cybercrime.

Follow @TheZDI for more info on upcoming Pwn2Own events and the latest threat research.

About Trend
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, our Trend cybersecurity platform protects hundreds of

security expertise, global threat research, and continuous innovation, our Trend 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, the 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 65 countries, Trend 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

---