Trend Micro Discovers Actively Exploited Vulnerability Affecting Millions of Users: Customers Already Protected

Bug allowing attackers to bypass critical protections uncovered by Trend's Zero Day Initiative

DALLAS, Feb. 13, 2024 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, announced its discovery of a vulnerability in Microsoft Windows Defender that is actively being exploited by cyberthreat group Water Hydra.

Trend discovered the vulnerability on December 31, 2023 and Trend customers have been automatically protected since January 1, 2024. Organizations are advised to take immediate action in response to the ongoing active exploitation of this vulnerability by cybercriminals.

This (CVE-2024-21412) is an active zero-day vulnerability that was disclosed by Trend Micro's Zero Day Initiative™ (ZDI) to Microsoft and is being published for the first time today.

Trend protects its customers by issuing virtual patches an average of 51 days before patches are released, including this zero-day for Microsoft. For all other vendors, the average time to actually protect their customers was 96 days. Trend estimates that customers who applied all virtual patches in 2023 saved an average of $1M for their enterprise.

Mark Houpt, CISO, Databank: "We have experienced first-hand the advantages of being under the protective umbrella of Trend Micro. Their unparalleled threat intelligence allows us to be proactively shielded against emerging threats. By implementing their virtual patches, we've managed to stay ahead of potential exploit attempts, securing our systems and allowing our customers to have confidence that their systems are secured long before official patches become available. It's a crucial part of our cybersecurity strategy, giving us peace of mind and significant cost savings in potential breach prevention."

When a new zero-day vulnerability is discovered, Trend responsibly discloses to the vendor. Trend customers then benefit from virtual patching to protect their systems from exploitation until an official patch can be applied.

Kevin Simzer, COO at Trend: "Zero-day vulnerabilities are an increasingly popular way for threat actors to achieve their goals. This is one reason we invest so deeply in threat intelligence, so we can keep our customers protected months before official vendor patches are released. We are proud to be creating a world with less cyber risk."

The critical risk is that vulnerabilities can be exploited by bad actors targeting any number of industries or organizations. This one is being actively exploited by the financially motivated APT group to compromise foreign exchange traders participating in the high-stakes currency trading market.

Specifically, it's used in a sophisticated zero-day attack chain to enable a Windows Defender SmartScreen bypass. Attacks are designed to infect victims with the DarkMe remote access trojan (RAT) for potential data theft and ransomware.

Using layers of defense to mitigate advanced threats, Trend's intrusion prevention system (IPS) capabilities delivered virtual patching by completely blocking the exploitation of CVE-2024-21412.

Trend Vision One™ automatically identifies critical vulnerabilities and provides visibility into all affected endpoints and their possible impact on an organization's overall risk. Trend's proactive approach to risk management reduces the need for last-minute reactive measures on "disclose day" and ensures customers are well-prepared to mitigate risks with confidence.

By contrast, organizations relying solely on a legacy endpoint detection and response (EDR) approach may be left exposed to the threat if their attackers use advanced techniques to avoid detection.

The power of the ZDI, the world's largest vendor-agnostic bug bounty program, to find and then feed intelligence into virtual patching has become increasingly important in light of two key trends identified by Trend:

- The zero-day vulnerabilities discovered by cybercrime groups are increasingly deployed in attack chains by nation-state groups like APT28, APT29, and APT40, broadening their reach.
- CVE-2024-21412 is itself a simple bypass of CVE-2023-36025, highlighting how easily APT groups can identify and circumvent narrow vendor patches.

To see more on the value of this news, please visit:*https://www.youtube.com/watch?v=yY08S4-aICA*

To read more technical information on how this occurred, please visit *https://www.trendmicro.com/en_us/*

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 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 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

---