Trend Micro | Newsroom

Trend Micro ZDI Surpasses 1000 Published Advisories in 1H 2023 In Continued Commitment to Coordinated Disclosure

Security leader to announce critical Microsoft zero-days at Black Hat USA 2023

DALLAS, Aug. 9, 2023 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, announced at Black Hat USA 2023 that its Zero Day Initiative program has published advisories addressing over 1000 unique vulnerabilities in 2023. The real-world impact if these vulnerabilities were to be weaponized would amount to time and financial losses of over 10 times the cost of prevention.

> Urgent action is needed to prioritize patching among researchers, cybersecurity vendors and cloud service providers.

"Our proactive investment of millions each year into vulnerability research and purchases saves billions in recovery for both our customers and the industry as a whole," said Kevin Simzer, COO at Trend. "A concerning trend is being documented of companies lacking transparency around vulnerability disclosure vendor patching, which pose a threat to the security of the digital world."

Today, Trend is calling for an end to silent patching – the practice of slowing or diluting public disclosure and documentation of vulnerabilities and patches. It is a major roadblock to fighting cybercrime but is all too common among major vendors and cloud providers.

During a session at Black Hat USA 2023, Trend Research representatives revealed that silent patching has become particularly common among cloud providers. Companies are more frequently refraining from assigning a Common Vulnerabilities and Exposures (CVE) ID for public documentation and are instead privately issuing patches.

The lack of transparency or version numbers for cloud services hinders risk assessment and deprives the wider security community of valuable information for enhancing overall ecosystem security.

At last year's Black Hat event, Trend warned of a growing number of incomplete or faulty patches and an increasing reluctance among vendors to deliver authoritative information on patches in plain language. The gap has since worsened, with some companies deprioritizing patching altogether, leaving their customers and industries exposed to unnecessary and increasing risk.

Urgent action is needed to prioritize patching, address vulnerabilities and foster collaboration among researchers, cybersecurity vendors and cloud service providers to fortify cloud-based services and protect users from potential risks.

Trend is committed to transparent vulnerability patching and aims to enhance security postures industry-wide through its Zero Day Initiative program. Through its commitment to transparent disclosure, Trend's ZDI issued today advisories on several zero-day vulnerabilities including:

ZDI-CAN-20784 Github (CVSS 9.9)

- This vulnerability allows remote attackers to escalate privileges on affected installations of Microsoft GitHub. Authentication is required to exploit this vulnerability
- The flaw exists within the configuration of Dev-Containers. The application does not enforce the privileged flag within a dev container configuration. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the hypervisor

ZDI-CAN-20771 Microsoft Azure (CVSS 4.4)

- This vulnerability allows remote attackers to disclose sensitive information on Microsoft Azure. An attacker must first obtain the ability to execute high-privileged code on the target environment in order to exploit this vulnerability
- The flaw exists within the handling of certificates. The issue results from the exposure of a resource to the wrong control sphere. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise.

To read more about Trend Micro's activities at Black Hat USA 2023, visit:
https://newsroom.trendmicro.com/2023-07-26-Trend-Micro-Deconstructs-Top-Cyberthreats-at-BlackHat-2023

For a full list of advisories published by Trend Micro's ZDI, visit:
https://www.zerodayinitiative.com/advisories/published/

Trend Micro's ZDI pioneered the vulnerability marketplace with a focus on disrupting attackers by legitimately purchasing vulnerability research that can then be disclosed to affected vendors to address before the information is made public.

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: Media Contact: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.ca/2023-08-09-Trend-Micro-ZDI-Surpasses-1000-Published-Advisories-in-1H-2023-In-Continued-Commitment-to-Coordinated-Disclosure