Zero Day Initiative pushes vendors to do better by changing its disclosure policy

DALLAS, Aug. 11, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today warned that a growing number of incomplete or faulty patches could be costing organizations upwards of $400,000 per update.

ZDI revealed policy changes to address declines in both the quality of patches and vendor communication with customers.

Speaking at Black Hat USA 2022, representatives from Trend Micro's Zero Day Initiative (ZDI)* revealed policy changes designed to address a significant decline in both the quality of patches and vendor communication with customers.

Click here to read more on the ZDI policy changes: https://www.zerodayinitiative.com/blog/2022/8/11/new-disclosure-timelines-for-bugs-from-faulty-patches

Brian Gorenc, senior director of vulnerability research and head of the ZDI , shared his perspective: "The ZDI has disclosed over 10,000 vulnerabilities to vendors since 2005, but we've never been more concerned about the state of security patches across the industry. Vendors that release inadequate patches with confusing advisories are costing their customers significant time and money and adding unnecessary business risk."

The ZDI has identified three primary issues resulting from vendors releasing faulty or otherwise incomplete patches:

- Due to flawed vendor practices, enterprises no longer have a clear view of the true risk to their networks.
- Due to incomplete and faulty updates, enterprises spend additional time and money patching what they've already patched.
- Due to falsely believing remediation has occurred, a failed patch results in more risk than no patch at all.

These scenarios effectively multiply the cost of patching because additional, corrective updates will be required to remediate a single vulnerability – wasting business resources and adding risk.

In addition, a growing reluctance among vendors to deliver authoritative information on patches in plain language leaves network defenders unable to accurately gauge their risk exposure.

The ZDI is therefore changing its disclosure policy for ineffective patches in a bid to drive industry-wide improvements. Moving forward, the standard 120-day timeline will be reduced for bugs believed to be the result of a bypassed security patch, as follows:

- 30 days for the most Critical-rated cases where exploitation is expected
- 60 days for Critical- and High-severity bugs where the Patch offers some protections
- 90 days for other severities where no imminent exploitation is expected

Even when patches are properly engineered, they can unintentionally increase risk by alerting threat actors to the underlying vulnerability. Few organizations' time-to-patch is quicker than the time-to-exploit. When patches are incomplete or faulty, the risk of compromise is multiplied.

Although patch costs differ between enterprises, Trend Micro calculated the cost of faulty patches with the following formula: **Total costs = f (T, HR, S, PF)** where T is Time spent on patch management, HR is Human Resources costs needed for patch management specialists, S is scope defining the number of applications to be patched, and PF is patch frequency, which can be every 2-3 week for some applications.

It is not uncommon for patch costs within medium-to-large enterprises to exceed six figures every month. Regardless of the formula used to calculate patch expenditures, applying multiple updates for the same vulnerability costs enterprises real time and money while exposing them to unneeded risk.

To better understand and mitigate these risks, Trend Micro recommends that organizations:

- Develop rigorous asset discovery and management programs
- Wherever possible, vote with their wallets for the most trustworthy vendors
- Conduct risk assessments that go beyond Patch Tuesday—for example, by monitoring for patch revisions and closely observing for changes to the threat landscape

**The ZDI is the world's largest vendor-agnostic bug bounty program, responsible for nearly 64% of all*

vulnerabilities disclosed in 2021.

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

---

https://newsroom.trendmicro.com/2022-08-11-Trend-Micro-Warns-of-Sharp-Decline-in-Quality-of-Security-Patches