Trend Micro's Zero Day Initiative Leads Vulnerability Disclosure Landscape in Independent Research

Analysis finds ZDI is largest contributor of vulnerability disclosures

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced the results of an independent and comprehensive study by IHS Markit, commissioned by Trend Micro. The report ranks Trend Micro and its Zero Day Initiative (ZDI) as the market leader in vulnerability disclosure[1]. The ZDI disclosed over half of all software flaws reported by vendors through coordinated disclosure in 2018.

The report, *Public Cybersecurity Vulnerability Market*, analyzed 12 organizations that collectively managed the disclosure of 1,752 CVE vulnerabilities in the 2018 calendar year. Trend Micro's ZDI accounted for 916 of these vulnerabilities, just over 52% of the total. This is nearly four times more than the number contributed by the next vendor, which disclosed 236.

"We know that vulnerabilities remain one of the biggest security weaknesses in modern organizations, enabling hackers to steal sensitive data and install malware which damages the bottom line and corporate reputation," said Brian Gorenc, director of vulnerability research for Trend Micro. "The ZDI has been leading the vulnerability disclosure market for nearly 15 years, and we continue to be the dominant player in the market, as this report proves. This is especially great news for Trend Micro TippingPoint customers, who are protected against exploits leveraging these bugs more than two months ahead of the public patch."

Of the 916 flaws disclosed by the ZDI, 64 were Critical, 598 were classified as High and 225 Medium importance. Accordingly, 72% of the vulnerabilities disclosed by the ZDI were considered to present significant risk to businesses. More than 500 of the vulnerabilities the ZDI disclosed were related to PDF software.

"Trend Micro's Zero Day Initiative disclosed a significant percentage of the total vulnerabilities patched this past year," said Tanner Johnson, senior analyst, connectivity and IoT at IHS Markit and lead analyst for the report. "In our research, we found that, not only did the ZDI disclose a lot of vulnerabilities, but also the identified software flaws could have resulted in significant business impacts if they were exploited."

Founded in 2005, Trend Micro's ZDI pioneered the creation of a white market in vulnerability disclosures, using bug bounty rewards to incentivize researchers. Since then, it has encouraged the responsible disclosure of more than 6,500 vulnerabilities and paid researchers more than $20 million in bounties.

To view the full report, please visit: https://cdn.ihsmarkit.com/www/pdf/1019/Vulnerability_Project_Whitepaper.pdf.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

###

[1] IHS Markit | Technology, now part of Informa Tech. Results are not an endorsement of Trend Micro Incorporated or its Zero Day Initiative. Any reliance on these results is at the third party’s own risk.

---

https://newsroom.trendmicro.ca/2019-12-03-Trend-Micros-Zero-Day-Initiative-Leads-Vulnerability-Disclosure-Landscape-in-Independent-Research