Trend Micro Plays Vital Role in Uncovering Critical Samba Bug

Defenders urged to rapidly patch vulnerability in popular open-source software

DALLAS, Feb. 2, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today confirmed its commitment to making the digital world safer by revealing the instrumental role its Zero Day Initiative (ZDI)* played in finding and reporting a critical vulnerability in the file sharing protocol Samba.

To find out more about the Samba flaw and how to mitigate its impact, please visit our blog here and technical support alert here.

"This latest vulnerability disclosure comes on the heels of the recent Log4j vulnerability and highlights the challenges many global security teams have in mitigating risk across a multitude of applications and open source software," said Jon Clay, vice president of threat intelligence at Trend Micro. "The good news is this was found during our Pwn2Own event, which means we had an opportunity to work with the developers to responsibly patch and disclose the vulnerabilities. So far, we have not heard of any in-the-wild attacks occurring."

Trend Micro's Pwn2Own events run regularly around the world, challenging contestants to find new vulnerabilities and exploits in widely used software and systems. They are part of a company-wide effort to enhance cybersecurity for customers and the entire online community through the ZDI and Trend Micro's own global threat intelligence team of thousands of researchers.

These efforts are increasingly important as organizations continue to digitally transform, expanding their attack surface and reliance on software – particularly open source components.

The vulnerability in question, CVE-2021-44142, was given a CVSS score of 9.9, illustrating its potentially critical impact on affected organizations. If exploited, the out-of-bounds heap read write bug could allow remote attackers to execute arbitrary code as root.

While no exploits of this vulnerability have been seen in the wild, the window in which affected organizations must patch critical new vulnerabilities before threat actors start exploiting them is increasingly short.

Trend Micro therefore calls on all organizations to patchCVE-2021-44142 or update to the latest Samba version as a matter of urgency.

** The vulnerability was originally disclosed at Pwn2OwnAustin 2021 by Nguyen Hoang Thach and Billy Jheng Bing-Jhong of STAR Labs. Lucas Leong of Trend Micro's ZDI discovered additional variants which were disclosed to Samba as part of this fix. The original issue was also independently found by Orange Tsai of DEVCORE. The ZDI is the world's largest vendor-agnostic bug bounty program. Since 2005, it has been making software safer by incentivizing researchers to find and responsibly disclose vulnerabilities to vendors.*

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

---