Daily threat bulletin

31 January 2025

Vulnerabilities

TeamViewer fixed a vulnerability in Windows client and host applications

Security Affairs - 30 January 2025 16:29

TeamViewer has patched a high-severity privilege escalation vulnerability affecting its Windows client and host applications. TeamViewer released security patches for a high-severity elevation of privilege vulnerability, tracked as CVE-2025-0065 (CVSS score of 7.8), in its remote access solutions for Windows.

VMware Patches High-Risk Flaws in Oft-Targeted Aria Operations Products

SecurityWeek - 30 January 2025 20:17

VMware calls attention to patches for multiple 'high-risk' security defects in its Aria Operations and Aria Operations for Logs products.

Threat actors and malware

New Syncjacking attack hijacks devices using Chrome extensions

BleepingComputer - 30 January 2025 10:33

A new attack called 'Browser Syncjacking' demonstrates the possibility of using a seemingly benign Chrome extension to take over a victim's device through the browser. [...]

Backdoor found in two healthcare patient monitors, linked to IP in China

BleepingComputer - 30 January 2025 19:31

The US Cybersecurity and Infrastructure Security Agency (CISA) is warning that Contec CMS8000 devices, a widely used healthcare patient monitoring device, include a backdoor that quietly sends patient data to a remote IP address and downloads and executes files on the device. [...]

Attackers Increase Use of HTTP Clients for Account Takeovers

Infosecurity Magazine - 30 January 2025 17:30

HTTP client tools used to compromise Microsoft 365 environments with 78% of tenants targeted in 2024

No need to RSVP: a closer look at the Tria stealer campaign

Securelist - 30 January 2025 09:00

Kaspersky GReAT experts discovered a new campaign targeting Android devices in Malaysia and Brunei with the Tria stealer to collect data from apps like WhatsApp and Gmail.

UK related

NCSC Calls on Vendors to Eradicate "Unforgivable" Vulnerabilities

Infosecurity Magazine - 30 January 2025 11:00

The UK's National Cyber Security Centre has released a new paper making it easier to assess if a flaw is "unforgivable"