Scottish Cyber Coordination Centre

Daily Threat Bulletin

26 November 2025

Vulnerabilities

CVE-2025-50165: This Windows JPEG Vulnerability Proves Detection Isn't Enough

Security Boulevard - 26 November 2025 00:38

The post CVE-2025-50165: This Windows JPEG Vulnerability Proves Detection Isn't Enough appeared first on Votiro.

Fluent Bit Vulnerabilities Expose Cloud Services to Takeover

SecurityWeek - 25 November 2025 14:45

Five flaws in the open source tool may lead to path traversal attacks, remote code execution, denial-of-service, and tag manipulation.

Threat actors and malware

CISA Warns of Active Spyware Campaigns Hijacking High-Value Signal and WhatsApp Users

The Hacker News - 25 November 2025 13:12

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday issued an alert warning of bad actors actively leveraging commercial spyware and remote access trojans (RATs) to target users of mobile messaging applications.

Morphisec warns StealC V2 malware spread through weaponized blender files

Security Affairs - 25 November 2025 16:15

Cybersecurity firm Morphisec reported that Russian threat actors are spreading StealC V2 infostealer via weaponized Blender files uploaded to 3D model marketplaces like CGTrader.

ToddyCat's New Hacking Tools Steal Outlook Emails and Microsoft 365 Access Tokens

The Hacker News - 25 November 2025 18:06

The threat actor known as ToddyCat has been observed adopting new methods to obtain access to corporate email data belonging to target companies, including using a custom tool dubbed TCSectorCopy.

Scottish Cyber Coordination Centre

HashJack attack shows AI browsers can be fooled with a simple '#'

The Register - 25 November 2025 18:58

Hashtag-do-whatever-I-tell-you Cato Networks says it has discovered a new attack, dubbed "HashJack," that hides malicious prompts after the "#" in legitimate URLs, tricking AI browser assistants into executing them while dodging traditional network and server-side defenses.