Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 November 2025

Vulnerabilities

CISA Confirms Exploitation of Recent Oracle Identity Manager Vulnerability

SecurityWeek - 24 November 2025 16:37

CISA has added CVE-2025-61757 to its Known Exploited Vulnerabilities (KEV) catalog.

Attackers deliver ShadowPad via newly patched WSUS RCE bug

Security Affairs - 24 November 2025 13:35

Attackers exploited a patched WSUS flaw (CVE-2025-59287) to gain access, use PowerCat for a shell, and deploy the ShadowPad malware.

New Fluent Bit Flaws Expose Cloud to RCE and Stealthy Infrastructure Intrusions

The Hacker News - 24 November 2025 21:33

Cybersecurity researchers have discovered five vulnerabilities in Fluent Bit, an open-source and lightweight telemetry agent, that could be chained to compromise and take over cloud infrastructures.

Threat actors and malware

ClickFix attack uses fake Windows Update screen to push malware

BleepingComputer - 24 November 2025 16:42

New ClickFix attack variants have been observed where threat actors trick users with a realistic-looking Windows Update animation in a full-screen browser page and hide the malicious code inside images.

Shai-Hulud malware infects 500 npm packages, leaks secrets on GitHub

BleepingComputer - 24 November 2025 10:32

Hundreds of trojanized versions of well-known packages such as Zapier, ENS Domains, PostHog, and Postman have been planted in the npm registry in a new Shai-Hulud supply-chain campaign.

Russian-linked Malware Campaign Hides in Blender 3D Files

Infosecurity Magazine - 24 November 2025 15:00

Morphisec has observed a new operation embedding StealC V2 malware in Blender project files, targeting users via 3D assets and launching a multi-stage infection chain.

Scottish Cyber Coordination Centre

Matrix Push C2 abuses browser notifications to deliver phishing and malware

Malwarebytes - 24 November 2025 16:43

Attackers can send highly realistic push notifications through your browser, including fake alerts that can lead to malware or phishing pages.