Scottish Cyber Coordination Centre

Daily Threat Bulletin

8 May 2026

Vulnerabilities

Ivanti EPMM CVE-2026-6973 RCE Under Active Exploitation Grants Admin-Level Access

The Hacker News - 08 May 2026 00:25

Ivanti is warning that a new security flaw impacting Endpoint Manager Mobile (EPMM) has been explored in limited attacks in the wild. The high-severity vulnerability, CVE-2026-6973 (CVSS score: 7.2), is a case of improper input validation affecting EPMM before versions 12.6.1.1, 12.7.0.1, and 12.8.0.1.

Palo Alto Networks firewall zero-day exploited for nearly a month

BleepingComputer - 07 May 2026 07:57

Palo Alto Networks warned customers that suspected state-sponsored hackers have been exploiting a critical-severity PAN-OS firewall zero-day vulnerability for nearly a month.

Cisco patches high-severity flaws enabling SSRF, code execution attacks

Security Affairs - 07 May 2026 15:15

Cisco released patches for multiple high-severity vulnerabilities affecting its enterprise products. Successful exploitation could allow code execution, server-side request forgery (SSRF), or denial-of-service attacks.

vm2 Node.js Library Vulnerabilities Enable Sandbox Escape and Arbitrary Code Execution

The Hacker News - 07 May 2026 10:45

A dozen critical security vulnerabilities have been disclosed in the vm2 Node.js library that could be exploited by bad actors to break out of the sandbox and execute arbitrary code on susceptible systems.

Attackers Could Exploit AI Vision Models Using Imperceptible Image Changes

SecurityWeek - 07 May 2026 14:45

Cisco's AI security researchers have analyzed ways to target vision-language models (VLMs) using pixel-level perturbation.

Scottish Cyber Coordination Centre

Threat actors and malware

New TCLBanker malware self-spreads over WhatsApp and Outlook

BleepingComputer - 07 May 2026 19:06

A new trojan named TCLBanker, which targets 59 banking, fintech, and cryptocurrency platforms, uses a trojanized MSI installer for Logitech AI Prompt Builder to infect systems.

PyPI Packages Deliver ZiChatBot Malware via Zulip APIs on Windows and Linux

The Hacker News - 07 May 2026 15:50

Cybersecurity researchers have discovered three packages on the Python Package Index (PyPI) repository that are designed to stealthily deliver a previously unknown malware family called ZiChatBot on Windows and Linux systems.

Australia warns of ClickFix attacks pushing Vidar Stealer malware

BleepingComputer - 07 May 2026 15:00

The Australian Cyber Security Center (ACSC) is warning organizations of an ongoing malware campaign using the ClickFix social engineering technique to distribute the Vidar Stealer info-stealing malware.

After Replacing TeamPCP Malware, 'PCPJack' Steals Cloud Secrets

darkreading - 07 May 2026 21:43

PCPJack makes innovative use of parquet files for stealthy, pre-validated target discovery as it canvasses multiple cloud environments.