Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 May 2026

Vulnerabilities

CC-4780 - Ivanti Releases Security Updates for High-Severity Vulnerabilities in Endpoint Manager Mobile (EPMM)

NHS Digital - 08 May 2026 15:58

Severity: Medium Two high-severity vulnerabilities in Ivanti EPMM could enable authenticated attackers to gain administrative access and execute arbitrary code Two high-severity vulnerabilities in Ivanti EPMM could enable authenticated attackers to gain administrative access and execute arbitrary code Updated: 08 May 2026

CC-4779 - Proof-of-Concept Exploit Released for Vulnerabilities in the Linux Kernel

NHS Digital - 08 May 2026 13:36

Severity: Medium CVE-2026-43284 and CVE-2026-43500 (dubbed as “Dirty Frag”), when chained together, could allow an unprivileged attacker to achieve root privileges on Linux distributions CVE-2026-43284 and CVE-2026-43500 (dubbed as “Dirty Frag”), when chained together, could allow an unprivileged attacker to achieve root privileges on Linux distributions Updated: 08 May 2026

CISA gives feds four days to patch Ivanti flaw exploited as zero-day

BleepingComputer - 08 May 2026 09:16

CISA has given U.S. federal agencies four days to secure their networks against a high-severity vulnerability in Ivanti Endpoint Manager Mobile (EPMM) exploited in zero-day attacks. [...]

New cPanel vulnerabilities could allow file access and remote code execution

Security Affairs - 10 May 2026 16:59

cPanel fixed three flaws that could allow file reads, code execution, and privilege escalation. No active exploitation has been reported yet. cPanel has released security updates to fix three vulnerabilities affecting cPanel & WHM that could allow attackers to read files, execute code, or escalate privileges on vulnerable systems. Below are the descriptions for these [...]

Ollama Out-of-Bounds Read Vulnerability Allows Remote Process Memory Leak

The Hacker News - 10 May 2026 19:11

Cybersecurity researchers have disclosed a critical security vulnerability in Ollama that, if successfully exploited, could allow a remote, unauthenticated attacker to leak its entire process memory.The out-of-bounds read flaw, which likely impacts over 300,000 servers globally, is tracked as CVE-2026-7482 (CVSS score: 9.1). It has been codenamed Bleeding Llama by Cyera.Ollama is a

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2026-42208 BerriAI LiteLLM SQL Injection Vulnerability.

Threat actors and malware

Hackers abuse Google ads, Claude.ai chats to push Mac malware

BleepingComputer - 10 May 2026 14:52

Attackers are abusing Google Ads and legitimate Claude.ai shared chats in an active malvertising campaign. Users searching for “Claude mac download” may come across sponsored search results that list claude.ai as the target website, but lead to instructions that install malware on their Mac. [...]

JDownloader site hacked to replace installers with Python RAT malware

BleepingComputer - 09 May 2026 16:27

The website for the popular JDownloader download manager was compromised earlier this week to distribute malicious Windows and Linux installers, with the Windows payload found deploying a Python-based remote access trojan. [...]

Fake OpenAI repository on Hugging Face pushes infostealer malware

BleepingComputer - 09 May 2026 11:26

A malicious Hugging Face repository that reached the platform’s trending list impersonated OpenAI’s “Privacy Filter” project to deliver information-stealing malware to Windows users. [...]

Official JDownloader site served malware to Windows and Linux users between May 6 and May 7

Security Affairs - 10 May 2026 13:33

JDownloader website was hacked to distribute malicious Windows and Linux installers carrying a Python RAT between May 6–7, 2026. JDownloader official website was compromised in a supply chain attack that replaced legitimate Windows and Linux installers with malicious files between May 6 and May 7, 2026. JDownloader is a free, open-source download management application designed [...]

New TCLBanker Malware Self-Spreads Over WhatsApp and Outlook

Security Boulevard - 10 May 2026 09:11

What happened Elastic Security Labs has documented a new Brazilian banking trojan called TCLBanker, tracked under campaign REF3076, that combines credential theft targeting 59 banking, fintech, and cryptocurrency platforms with self-spreading worm modules that propagate the malware autonomously through victims’ own WhatsApp and Microsoft Outlook accounts. The malware is delivered through a trojanized MSI installer [...]The post

Scottish Cyber Coordination Centre

New TCLBanker Malware Self-Spreads Over WhatsApp and Outlook appeared first on CISO Whisperer.

Cyberattack Hits Canvas System Used by Thousands of Schools as Finals Loom

SecurityWeek - 08 May 2026 11:43

A system that thousands of schools and universities use went offline due to a cyberattack, creating chaos as students tried to study for finals.