Scottish Cyber Coordination Centre

Daily Threat Bulletin

26 October 2026

Vulnerabilities

CISA Flags Two Actively Exploited Critical Flaws in Collabora Online and Arista VeloCloud

The Hacker News - 24 October 2026 12:55

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added two vulnerabilities impacting Collabora Online Built-in CODE Server and Arista VeloCloud Orchestrator (VCO) to its Known Exploited Vulnerabilities (KEV), citing reports of active exploitation in the wild.

PHP Warns of New Code Execution Flaw Days After PHP2Shell Patches

Security Affairs - 23 October 2026 19:07

PHP has warned of a new code execution vulnerability, tracked as CVE-2026-115560, just two days after releasing emergency patches for the critical PHP2Shell flaws.

Critical Flaw in Python's Popular Pillow Image Library Allows Code Execution via a Crafted Image

The Hacker News - 23 October 2026 16:06

Pillow, the most widely used image library for Python, can be made to run operating system commands on a server by specifying the name of a file it is told to open.The flaw, CVE-2026-112900, is in the way Pillow handles EPS images, which it opens by passing the file's name to Ghostscript, a separate program it runs to turn the image into pixels, without checking the name first.

HPE patches eight max severity RCE and auth bypass AOS flaws

BleepingComputer - 23 October 2026 09:48

Hewlett Packard Enterprise (HPE) released security updates to patch 72 vulnerabilities in the Aruba Operating System (ArubaOS), including eight maximum-severity authentication bypass and code execution issues.

Ruby Fixes Three Regex Engine Bugs Responsible for Four Critical GitLab RCE Flaws

The Hacker News - 24 October 2026 00:24

Ruby has released versions 4.0.9, 3.4.12, and 3.3.13 to fix three bugs in Onigmo, the regular expression engine built into the language. The bugs lie behind four critical security flaws that GitLab patched over the past month.

Scottish Cyber Coordination Centre

Atlassian Patches 75 Flaws in Data Center and Server Products

SecurityWeek - 23 October 2026 08:54

Atlassian's October bulletin lists 176 vulnerability entries, including 14 critical-severity issues, all in third-party components.

Threat actors and malware

Russia-Linked Hackers Used New Mesh Network Backdoor in Destructive Ukraine Attack

The Hacker News - 23 October 2026 17:41

The Russian state-sponsored hacking group Sandworm teamed up with another threat actor to carry out a destructive wiping attack targeting a Ukrainian logistics company last year.

Hackers Breach Enterprise Firewalls and VPNs, Exposing Over 70,000 Credentials

The Hacker News - 23 October 2026 20:20

Cybersecurity researchers have disclosed details of a large-scale campaign that has targeted exposed network edge devices such as Fortinet FortiGate and Palo Alto Networks GlobalProtect firewalls.

Mirai Botnet Operators Join PHP2Shell Attacks as ASLR Bypass Exploits Emerge

SecurityWeek - 23 October 2026 13:45

Researchers tie PHP2Shell attempts to a Mirai botnet and show an ASLR bypass, but no successful compromise has been confirmed yet.

China APT Uses AI Pentest Tool Artex in ConnectWise Attacks

SecurityWeek - 23 October 2026 11:31

The state-sponsored hackers targeted hundreds of organizations and gained privileged access to some environments.

Microsoft Teams to get AI-powered, context-aware phishing detection

BleepingComputer - 23 October 2026 15:54

Microsoft has announced plans to add AI-powered phishing detection to Teams messages starting in early November 2026.

Malicious File in Downloads Folder Tries to Trick AI Coding Agent Into Installing Malware

The Hacker News - 26 October 2026 12:33

A malicious instruction file sitting in a developer's Downloads folder tried to make their AI coding agent install a known-malicious npm package, security firm Forever Security said in a report published last week.

Scottish Cyber Coordination Centre

Widespread Token-Spraying Attacks Target Microsoft 365 Accounts For Email Compromise

Infosecurity Magazine - 23 October 2026 11:30

Security researchers identified attempts to access corporate networks which have been linked to a major Microsoft 365-targeted BEC campaign using phishing, stolen session tokens and social engineering.