Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 April 2026

Vulnerabilities

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-2026-1340 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability

Anthropic's Claude Mythos Finds Thousands of Zero-Day Flaws Across Major Systems

The Hacker News - 08 April 2026 15:46

Artificial Intelligence (AI) company Anthropic announced a new cybersecurity initiative called Project Glasswing that will use a preview version of its new frontier model, Claude Mythos, to find and address security vulnerabilities.

Critical Vulnerability in Ninja Forms Exposes WordPress Sites

Infosecurity Magazine - 08 April 2026 16:10

Ninja Forms File Upload RCE via unauthenticated arbitrary file upload; update to 3.3.27 immediately.

Data Leakage Vulnerability Patched in OpenSSL

SecurityWeek - 08 April 2026 16:37

A total of seven vulnerabilities, most of which can be exploited for DoS attacks, have been patched in OpenSSL.

Threat actors and malware

Hackers use pixel-large SVG trick to hide credit card stealer

BleepingComputer - 08 April 2026 19:34

A massive campaign impacting nearly 100 online stores using the Magento e-commerce platform hides credit card-stealing code in a pixel-sized Scalable Vector Graphics (SVG) image.

Scottish Cyber Coordination Centre

New macOS stealer campaign uses Script Editor in ClickFix attack

BleepingComputer - 08 April 2026 15:55

A new campaign delivering the Atomic Stealer malware to macOS users abuses the Script Editor in a variation of the ClickFix attack that tricked users into executing commands in Terminal.

Russia-linked APT28 uses PRISMEX to infiltrate Ukraine and allied infrastructure with advanced tactics

Security Affairs - 08 April 2026 21:23

Russia-linked group APT28 (aka UAC-0001, aka Fancy Bear, Pawn Storm, Sofacy Group, Sednit, BlueDelta, and STRONTIUM) is running a spear-phishing campaign against Ukraine and its allies, deploying a new malware suite called PRISMEX.

N. Korean Hackers Spread 1,700 Malicious Packages Across npm, PyPI, Go, Rust

The Hacker News - 08 April 2026 14:17

The North Korea-linked persistent campaign known as Contagious Interview has spread its tentacles by publishing malicious packages targeting the Go, Rust, and PHP ecosystems.

Masjesu Botnet Emerges as DDoS-for-Hire Service Targeting Global IoT Devices

The Hacker News - 08 April 2026 23:00

Cybersecurity researchers have lifted the curtain on a stealthy botnet that's designed for distributed denial-of-service (DDoS) attacks. Called Masjesu, the botnet has been advertised via Telegram as a DDoS-for-hire service since it first surfaced in 2023.

Google: New UNC6783 hackers steal corporate Zendesk support tickets

BleepingComputer - 08 April 2026 18:46

A threat actor tracked as UNC6783 is compromising business process outsourcing (BPO) providers to gain access to high-value companies across multiple sectors.

US Disrupts Russian Espionage Operation Involving Hacked Routers and DNS Hijacking

SecurityWeek - 08 April 2026 11:54

The APT28 threat group exploited vulnerable TP-Link and MikroTik routers to conduct adversary-in-the-middle (AitM) attacks.

UK incidents

NHS Scotland-linked domains caught serving pr0n and dodgy sports streams

The Register - 08 April 2026 11:00

Multiple domains belonging to Scottish healthcare providers have been hijacked and are now pushing links to adult content and illegal sports streams, according to a researcher.