Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 April 2026

Vulnerabilities

CC-4772 - Cisco Releases Security Advisories for Critical Vulnerabilities in Identity Services Engine

NHS Digital - 16 April 2026 14:03

Severity: Medium An authenticated attacker could exploit the vulnerabilities to achieve remote code execution An authenticated attacker could exploit the vulnerabilities to achieve remote code execution Updated: 16 Apr 2026

Recently leaked Windows zero-days now exploited in attacks

BleepingComputer - 17 April 2026 03:14

Threat actors are exploiting three recently disclosed Windows security vulnerabilities in attacks aimed at gaining SYSTEM or elevated administrator permissions. [...]

New Microsoft Defender “RedSun” zero-day PoC grants SYSTEM privileges

BleepingComputer - 16 April 2026 17:19

A researcher known as “Chaotic Eclipse” has published a proof-of-concept exploit for a second Microsoft Defender zero-day, dubbed “RedSun,” in the past two weeks, protesting how the company works with cybersecurity researchers. [...]

Hackers exploit Marimo flaw to deploy NKAbuse malware from Hugging Face

BleepingComputer - 16 April 2026 13:58

Hackers are exploiting a critical vulnerability in Marimo reactive Python notebook to deploy a new variant of NKAbuse malware hosted on Hugging Face Spaces. [...]

Apache ActiveMQ CVE-2026-34197 Added to CISA KEV Amid Active Exploitation

The Hacker News - 17 April 2026 09:52

A recently disclosed high-severity security flaw in Apache ActiveMQ Classic has come under active exploitation in the wild, per the U.S. Cybersecurity and Infrastructure Security Agency (CISA).To that end, the agency has added the vulnerability, tracked as CVE-2026-34197 (CVSS score: 8.8), to its Known Exploited Vulnerabilities (KEV) catalog, requiring Federal Civilian

Threat actors and malware

ZionSiphon malware designed to sabotage water treatment systems

BleepingComputer - 16 April 2026 19:04

A new malware called ZionSiphon, specifically designed for operational technology, is targeting water treatment and desalination environments to sabotage their operations. [...]

New ATHR vishing platform uses AI voice agents for automated attacks

BleepingComputer - 16 April 2026 11:09

A new cybercrime platform called ATHR can harvest credentials via fully automated voice phishing attacks that use both human operators and AI agents for the social engineering phase. [...]

AI platform n8n abused for stealthy phishing and malware delivery

Security Affairs - 16 April 2026 14:57

Attackers abuse AI automation platform n8n to run phishing campaigns, deliver malware, and evade security by using trusted infrastructure. Threat actors are exploiting the popular AI workflow automation platform n8n to launch advanced phishing campaigns, deliver malware, and collect device data through automated emails. By using trusted infrastructure, they can bypass traditional security controls and [...]

Obsidian Plugin Abuse Delivers PHANTOMPULSE RAT in Targeted Finance, Crypto Attacks

The Hacker News - 16 April 2026 16:50

A “novel” social engineering campaign has been observed abusing Obsidian, a cross-platform note-taking application, as an initial access vector to distribute a previously undocumented Windows remote access trojan called PHANTOMPULSE in attacks targeting individuals in the financial and cryptocurrency sectors.

North Korea targets macOS users in latest heist

The Register - 16 April 2026 19:20

Social engineering: ‘low-cost, hard to patch, and scales well’ North Korean criminals set on stealing Apple users’ credentials and cryptocurrency are using a combination of social engineering and a fake Zoom software update to trick people into manually running malware on their own computers, according to Microsoft....