Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 April 2026

Vulnerabilities

New FortiClient EMS flaw exploited in attacks, emergency patch released

BleepingComputer - 05 April 2026 15:45

Fortinet has released an emergency weekend security update for a new critical FortiClient Enterprise Management Server (EMS) vulnerability that is actively exploited in attacks.

36 Malicious npm Packages Exploited Redis, PostgreSQL to Deploy Persistent Implants

The Hacker News - 05 April 2026 11:37

Cybersecurity researchers have discovered 36 malicious packages in the npm registry that are disguised as Strapi CMS plugins but come with different payloads to facilitate Redis and PostgreSQL exploitation, deploy reverse shells, harvest credentials, and drop a persistent implant.

New Progress ShareFile Bugs Let Attackers Take Over Servers Without Logging In

Security Boulevard - 05 April 2026 15:18

New Progress ShareFile bugs could let attackers take over exposed on-premises servers without logging in by chaining an authentication bypass with remote code execution.

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-31277 Apple Multiple Products Buffer Overflow Vulnerability
CVE-2025-32432 Craft CMS Code Injection Vulnerability
CVE-2025-43510 Apple Multiple Products Improper Locking Vulnerability
CVE-2025-43520 Apple Multiple Products Classic Buffer Overflow Vulnerability
CVE-2025-54068 Laravel Livewire Code Injection Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors.

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers exploit React2Shell in automated credential theft campaign

BleepingComputer - 05 April 2026 11:17

Hackers are running a large-scale campaign to steal credentials in an automated way after exploiting React2Shell (CVE-2025-55182) in vulnerable Next.js apps.

$285 Million Drift Hack Traced to Six-Month DPRK Social Engineering Operation

The Hacker News - 06 April 2026 00:55

Drift has revealed that the April 1, 2026, attack that led to the theft of $285 million was the culmination of a months-long targeted and meticulously planned social engineering operation undertaken by the Democratic People's Republic of Korea (DPRK).

Hackers Spread Vidar and GhostSocks Malware Through Claude Code Leak

Security Boulevard - 05 April 2026 15:17

Hackers are weaponizing the leaked Claude Code source to spread Vidar and GhostSocks malware through malicious repositories that impersonate the exposed codebase. The campaign followed Anthropic's March 31 packaging error, which exposed the source code for Claude Code in a public npm package through a JavaScript source map file.

Russian Intelligence Services Target Commercial Messaging Application Accounts

CISA Advisories -

CISA and the Federal Bureau of Investigation released a Public Service Announcement (PSA) warning about ongoing phishing campaigns by cyber actors associated with the Russian Intelligence Services targeting commercial messaging applications (CMAs). These campaigns aim to bypass encryption to compromise to individual user accounts with targets including current and former U.S. government officials, military personnel, political figures, and journalists.

UK related

What capabilities do NHIs bring to cybersecurity

Security Boulevard - 05 April 2026 22:00

Non-Human Identities (NHIs) serve as the fundamental building blocks for securing machine-to-machine interactions.