Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 April 2026

Vulnerabilities

Hackers Exploit CVE-2025-55182 to Breach 766 Next.js Hosts, Steal Credentials

The Hacker News - 03 April 2026 02:00

A large-scale credential harvesting operation has been observed exploiting the React2Shell vulnerability as an initial infection vector to steal database credentials, SSH private keys, Amazon Web Services (AWS) secrets, shell command history, Stripe API keys, and GitHub tokens at scale.

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-2026-3502 TrueConf Client Download of Code Without Integrity Check Vulnerability

Cisco fixed critical and high-severity flaws

Security Affairs - 02 April 2026 18:04

Cisco released patches for two critical and six high-severity vulnerabilities. These flaws could let attackers bypass authentication, execute malicious code, escalate privileges, and access sensitive information.

Apple Expands iOS 18.7.7 Update to More Devices to Block DarkSword Exploit

The Hacker News - 02 April 2026 13:39

Apple on Wednesday expanded the availability of iOS 18.7.7 and iPadOS 18.7.7 to a broader range of devices to protect users from the risk posed by a recently disclosed exploit kit known as DarkSword.

New Progress ShareFile flaws can be chained in pre-auth RCE attacks

BleepingComputer - 02 April 2026 10:33

Two vulnerabilities in Progress ShareFile, an enterprise-grade secure file transfer solution, can be chained to enable unauthenticated file exfiltration from affected environments.

Critical Vulnerability in Claude Code Emerges Days After Source Leak

SecurityWeek - 02 April 2026 19:00

Within days of each other, Anthropic first leaked the source code to Claude Code, and then a critical vulnerability was found by Adversa AI.

Scottish Cyber Coordination Centre

Threat actors and malware

NCSC Issues Security Alert Over Hackers Targeting WhatsApp and Signal Accounts

Infosecurity Magazine - 02 April 2026 15:15

The UK's cybersecurity agency offered advice to "high-risk' individuals" on how to protect against social engineering and cyber-attacks.

Threat actor UAC-0255 impersonate CERT-UA to spread AGEWHEEZE malware via phishing

Security Affairs - 02 April 2026 15:02

Threat actors impersonated CERT-UA to send phishing emails with AGEWHEEZE malware, tricking victims into installing a fake "security tool." A threat actor, tracked as UAC-0255, impersonated CERT-UA in a phishing campaign, sending emails to about 1 million users.

Medtech giant Stryker fully operational after data-wiping attack

BleepingComputer - 02 April 2026 10:28

Stryker Corporation, one of the world's leading medical technology companies, says it's fully operational three weeks after many of its systems were wiped out in a cyberattack claimed by the Iranian-linked Handala hacktivist group.