Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 March 2026

Vulnerabilities

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.

Trivy vulnerability scanner breach pushed infostealer via GitHub Actions

BleepingComputer - 21 March 2026 14:30

The Trivy vulnerability scanner was compromised in a supply-chain attack by threat actors known as TeamPCP, which distributed credential-stealing malware through official releases and GitHub Actions. [...]

CISA orders feds to patch max-severity Cisco flaw by Sunday

BleepingComputer - 20 March 2026 12:09

The Cybersecurity and Infrastructure Security Agency (CISA) has ordered federal agencies to patch a maximum-severity vulnerability, CVE-2026-20131, in Cisco Secure Firewall Management Center (FMC) by Sunday, March 22. [...]

Oracle fixes critical RCE flaw CVE-2026-21992 in Identity Manager

Security Affairs - 22 March 2026 16:37

Oracle fixed a critical severity flaw, tracked as CVE-2026-21992, enabling unauthenticated remote code execution in Identity Manager. Oracle released security updates to address a critical vulnerability, tracked as CVE-2026-21992 (CVSS score of 9.8), affecting Identity Manager and Web Services Manager.

PolyShell flaw exposes Magento and Adobe Commerce to file upload attacks

Security Affairs - 21 March 2026 11:09

Sansec found a Magento and Adobe Commerce REST API flaw, named PolyShell, which allows unauthenticated file uploads and possible XSS in older versions. Sansec disclosed a critical flaw in the Magento and Adobe Commerce REST API that allows attackers to upload executable files without authentication.

Scottish Cyber Coordination Centre

Hackers Exploit CVE-2025-32975 (CVSS 10.0) to Hijack Unpatched Quest KACE SMA Systems

The Hacker News - 23 March 2026 12:45

Threat actors are suspected to be exploiting a maximum-severity security flaw impacting Quest KACE Systems Management Appliance (SMA), according to Arctic Wolf.

Threat actors and malware

VoidStealer malware steals Chrome master key via debugger trick

BleepingComputer - 22 March 2026 11:32

An information stealer called VoidStealer uses a new approach to bypass Chrome's Application-Bound Encryption (ABE) and extract the master key for decrypting sensitive data stored in the browser. [...]

Microsoft Azure Monitor alerts abused for callback phishing attacks

BleepingComputer - 21 March 2026 11:09

Microsoft Azure Monitor alerts are being abused to send callback phishing emails that impersonate warnings from the Microsoft Security Team about unauthorized charges on your account. [...]

Russia-linked actors target WhatsApp and Signal in phishing campaign

Security Affairs - 22 March 2026 20:21

Russia-linked actors target WhatsApp and Signal accounts of officials and journalists via phishing, gaining access to messages and contacts. Threat actors linked to Russian Intelligence Services are running phishing campaigns to hijack high-value accounts on messaging apps like WhatsApp and Signal, the FBI warns.

7,500+ Magento sites defaced in global hacking campaign

Security Affairs - 20 March 2026 23:21

Hackers defaced 7,500 Magento sites since Feb 27, uploading files across 15,000 hostnames, mostly opportunistic attacks. Since February 27, a large-scale campaign has defaced over 7,500 Magento sites, targeting e-commerce platforms, global brands, and government services.

Trivy Supply Chain Attack Triggers Self-Spreading CanisterWorm Across 47 npm Packages

The Hacker News - 21 March 2026 14:55

The threat actors behind the supply chain attack targeting the popular Trivy scanner are suspected to be conducting follow-on attacks that have led to the compromise of a large number of npm packages with a previously undocumented self-propagating worm dubbed CanisterWorm.

Scottish Cyber Coordination Centre

Interlock Ransomware Targets Cisco Enterprise Firewalls

darkreading - 20 March 2026 14:00

The ransomware gang, known for double-extortion attacks, had access to a critical Cisco firewall vulnerability weeks before it was publicly disclosed.

UK related

Jaguar Land Rover's cyber bailout sets worrying precedent, watchdog warns

The Register - 20 March 2026 13:42

Lack of clear criteria risks encouraging firms to lean on state support instead of worrying about insurance The UK's cyber watchdog has warned that the government's £1.5 billion bailout of Jaguar Land Rover (JLR) risks setting a troubling precedent for how Britain handles major cyber crises....

NCA Boss Warns That Teens Are Being "Radicalized" Into Cybercrime Online

Infosecurity Magazine - 20 March 2026 10:40

The National Crime Agency's director general warns that technology is rapidly reshaping crime