Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 June 2026

Vulnerabilities

Cisco Unified CM flaw CVE-2026-20230 now exploited in attacks

BleepingComputer - 23 June 2026 18:48

A high-severity SSRF vulnerability, tracked as CVE-2026-20230, in Cisco Unified Communications Manager Server is now being exploited in attacks.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

CVE-2025-67038 Lantronix EDS5000 Code Injection Vulnerability

CVE-2026-34908 Ubiquiti UniFi OS Improper Access Control Vulnerability

CVE-2026-34909 Ubiquiti UniFi OS Path Traversal Vulnerability

CVE-2026-34910 Ubiquiti UniFi OS Improper Input Validation Vulnerability

Eight-Year-Old Samsung KNOX Flaw Exposed Millions of Galaxy Devices to Kernel Attacks

SecurityWeek - 23 June 2026 14:00

The high-severity use-after-free vulnerability in Samsung's KNOX security framework affected Android-powered Galaxy devices from the S9 through S25.

DifyTap: Four Bugs Put over 1 million AI Apps at Risk

Security Affairs - 23 June 2026 18:01

Four flaws in Dify exposed cross-tenant data, documents and AI conversations. Two critical bugs enabled unauthenticated access and data theft.

OpenAI Expands Daybreak to Help Defenders Patch Flaws

Infosecurity Magazine - 23 June 2026 15:15

OpenAI expanded Daybreak with a full GPT-5.5-Cyber release to help defenders patch software flaws.

Scottish Cyber Coordination Centre

Threat actors and malware

FortiBleed Targeted FortiGate Firewalls in 110 Million-Credential Harvesting Operation

The Hacker News - 24 June 2026 00:50

A Russian-speaking initial access broker (IAB) driven by financial gain is assessed to be behind a large-scale credential-harvesting operation known as FortiBleed that has targeted over 430,000 FortiGate firewalls globally.

New macOS ClickFix attack silently mounts DMGs to push infostealer

BleepingComputer - 23 June 2026 15:30

A new macOS ClickFix campaign is using Terminal commands to silently download, mount, and launch info-stealing malware from malicious disk image (DMG) files.

ShapedPlugin Supply Chain Attack Backdoors Pro Plugin Updates

Security Affairs - 23 June 2026 09:22

Attackers backdoored ShapedPlugin Pro updates, deploying malware that steals credentials, 2FA secrets, and grants full site access. If you installed a ShapedPlugin Pro plugin between April and June 2026 and kept it updated, your site may be compromised.

Eight-Year-Old Samsung KNOX Flaw Exposed Millions of Galaxy Devices to Kernel Attacks

SecurityWeek - 23 June 2026 14:00

The high-severity use-after-free vulnerability in Samsung's KNOX security framework affected Android-powered Galaxy devices from the S9 through S25.

Data Exposure Flaws Threaten Dify AI Platform Used by 1 Million Apps

SecurityWeek - 23 June 2026 16:36

Attackers could abuse Dify's multi-tenant cloud service to read private chats, preview other tenants' documents, and reach internal APIs.

Five Eyes Group Issues Urgent Call to Tackle Frontier AI Threats

Infosecurity Magazine - 23 June 2026 09:30

The Five Eyes Alliance has published a rare call to action for organizations facing AI threats.

Russian Initial Access Broker Behind FortiBleed Campaign

SecurityWeek - 23 June 2026 11:30

Using a custom sniffer, the threat actor has captured over 110 million credentials since at least February 2026.

Scottish Cyber Coordination Centre

UK incidents

Scattered Spider Teens Convicted of TfL Cyber-Attack

Infosecurity Magazine - 23 June 2026 10:29

Two young British men have pleaded guilty to hacking Transport for London as part of a Scattered Spider plot.