Scottish Cyber Coordination Centre

Daily Threat Bulletin

26 June 2026

Vulnerabilities

Cisco Catalyst SD-WAN Zero-Day CVE-2026-20245 Exploited to Gain Root Access

The Hacker News - 25 June 2026 12:16

An unknown threat actor exploited a recently disclosed high-severity security flaw impacting Cisco Catalyst SD-WAN as a zero-day at least two months before it was publicly disclosed, according to new findings from Google-owned Mandiant.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

CVE-2026-12569 PTC Windchill and FlexPLM Improper Input Validation Vulnerability

CVE-2026-20230 Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability

Lantronix Serial-to-IP Converter Flaw Exploited in Attacks After OT Threat Warning

SecurityWeek - 25 June 2026 12:23

The exploited flaw, CVE-2025-67038, is one of the vulnerabilities disclosed in April as part of the BRIDGE:BREAK research project.

Curl Fixes a 25-Year-Old Bug in Its Largest CVE Release Yet

Security Affairs - 25 June 2026 20:20

Curl fixed 18 vulnerabilities, including a 25-year-old bug, with issues spanning auth bypass, memory safety, and host validation in libcurl.

macOS Flaw Lets Standard Users Disable EDR and MDM

Infosecurity Magazine - 25 June 2026 12:00

macos-xpc-flaw-disable-edr-mdm-standard-user-xm-cyber.

GitLab Patches Code Execution, Information Disclosure Vulnerabilities

SecurityWeek - 25 June 2026 12:10

The latest GitLab CE/EE updates address 13 vulnerabilities, including three high-severity defects.

Scottish Cyber Coordination Centre

Chrome 149 Update Resolves 18 Severe Vulnerabilities

SecurityWeek - 25 June 2026 08:56

More than half of the bugs are use-after-free defects, which can potentially lead to remote code execution.

Threat actors and malware

New Gaslight macOS Malware Uses Prompt Injection to Disrupt AI-Assisted Analysis

The Hacker News - 25 June 2026 15:53

A previously undocumented Rust-based macOS implant and information stealer has been found to embed a prompt injection payload designed to trick a malware analyst's artificial intelligence (AI) tools and trick it into aborting or refusing an analysis of the artifact.

Inside Mistic, the New Stealth Backdoor in Ransomware Intrusions

Security Affairs - 25 June 2026 16:07

Mistic is a stealthy backdoor used by KongTuke-linked actors to keep long-term access in ransomware-targeted networks. Mistic is the kind of backdoor that tells you the operator wants time, not noise.

Bluekit phishing kit adopts browser-in-the-middle for login theft

BleepingComputer - 25 June 2026 12:00

The Bluekit phishing-as-a-service platform continues to evolve with nearly 70 new hostnames identified over the past week and by adding browser-in-the-middle capabilities for improved data theft.

Russian APT 'Gamaredon' Upgrades Its Arsenal, Requiring New Defenses

darkreading - 25 June 2026 22:12

The FSB state-sponsored operation has gotten a lot better at loading its malware and hiding its servers.

Order-tracking app Shop abused to push callback phishing attacks

BleepingComputer - 25 June 2026 16:45

Threat actors are increasingly abusing Shop, the order-tracking app from Shopify, by adding fake purchase receipts in users' order histories to trick them into providing sensitive data or installing remote access software.