Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 August 2026

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog

CISA - 19 August 2026 12:00

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

CVE-2026-64849 MLflow Server-Side Request Forgery Vulnerability

Critical RCE flaw in Windows IKE Extension now actively exploited

Bleeping Computer - 19 August 2026 06:12

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned that hackers are exploiting a critical-severity remote code execution (RCE) flaw in the Windows Internet Key Exchange (IKE) Service Extensions component.

Critical Citrix NetScaler Flaw Lets Remote Attackers Bypass Authentication Without Credentials

Cyber Security News - 19 August 2026 16:56

Cloud Software Group has issued a critical security bulletin warning customers of two serious vulnerabilities affecting NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway).

943 Patches Rolled Out With Oracle's August 2026 Security Update

Security Week - 19 August 2026 09:14

The fixes resolve over 1,000 vulnerabilities across two dozen products, including over 460 remotely exploitable bugs.

Chrome, Firefox Updates Patch Dozens of Vulnerabilities

Security Week - 19 August 2026 08:19

The bugs could lead to code execution, privilege escalation, sandbox escape, and information disclosure.

Scottish Cyber Coordination Centre

Threat actors and malware

Password spraying attacks surge 155x as hackers exploit MFA gaps

Bleeping Computer - 19 August 2026 10:00

Huntress observed a 155x increase in password spraying attacks in H1 2026, including a campaign that generated more than 81 million login attempts in two weeks.

Microsoft Tracks MacSync Stealer by Its Behavior, Not Its Domains

Security Affairs - 19 August 2026 08:55

Microsoft tracked over 30 MacSync Stealer domains by focusing on behavioral patterns, revealing a campaign targeting passwords, keys, wallets and other data. Domain blocking is a losing game when the thing you're blocking can register a new domain faster than you can add it to a list.

StopAndProtect Uses Nearly 2,000 Hacked WordPress Sites to Spread Malware and Steal Data

The Hacker News - 19 August 2026 16:55

Cybersecurity researchers have flagged a global cybercrime operation that abuses thousands of hacked WordPress websites as infrastructure to disseminate malware, commandeer infected hosts, store stolen documents, screenshots, and activity logs created to track the status of the activity.

Rogue ransomware affiliate poses as recovery firm to steal payments

Bleeping Computer - 19 August 2026 16:59

A suspected ransomware affiliate is posing as a ransomware recovery service called "Ransom Busters," contacting the victims before the attacks become public and claiming to be able to provide decryption keys and delete stolen data for a fee.

The long tail of Clop's PTC hack is just beginning to emerge

CyberScoop - 19 August 2026 14:30

The data theft extortion group likely compromised a critical vulnerability affecting PTC's product lifecycle management software in June, a month before it sent threatening emails to victims.

SilkParasite Espionage Campaign Targets Central Asian Governments with Five New RATs

The Hacker News - 19 August 2026 18:42

A previously unreported cyber espionage operation dubbed SilkParasite has been observed targeting government bodies in Central Asia. The intrusion set makes use of seven remote access tool (RAT) families, five of which have never been previously documented: DriveSilkRAT, CookiETagRAT, NomadRAT, GoginRAT, and NodeEdgeRAT.

Scottish Cyber Coordination Centre

Inside Operation CameraSwarm: How One Actor Took Over 14,000 Dahua Cameras

Security Affairs - 19 August 2026 17:35

An exposed operator directory reveals how one actor compromised 14,000+ Dahua cameras across Ukraine and Russia, no password needed for most. A researcher discovered an exposed directory containing the tools of an attacker who compromised more than 14,000 Dahua cameras between June 17 and July 22, 2026, mainly in Ukraine and Russia.