Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 September 2026

Vulnerabilities

Critical ScreenConnect flaw now actively exploited in attacks

BleepingComputer - 16 September 2026 08:14

Attackers now exploit a critical-severity ConnectWise ScreenConnect vulnerability in the wild, according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Attackers Exploit Issabel Framework Flaw Enabling Unauthenticated OS Command Execution

The Hacker News - 16 September 2026 22:20

A critical security flaw in Issabel Framework, a web-based framework for the open-source unified communications PBX software, has come under active exploitation.

Parallels Desktop Flaw Lets Non-Admin Mac Users Gain Root, but Intel Macs Can't Install Fix

The Hacker News - 16 September 2026 19:44

Parallels Desktop for Mac has a flaw that lets an ordinary local account run code as root, the highest level of access on a Mac, software company JFrog said this week.

Acronis cPanel Backup Plugin Vulnerability Exploited in Targeted Attacks

The Hacker News - 16 September 2026 17:38

Acronis has warned that a high-severity security flaw in its Backup plugin for cPanel and Web Host Manager (WHM) deployments has been exploited in the wild.

Unauthenticated RCE Flaws Could Expose 200,000+ WordPress Sites to Takeover

SecurityWeek - 16 September 2026 12:32

Vulnerabilities in The Events Calendar can provide attackers with remote code execution capabilities. The Unauthenticated RCE Flaws Could Expose 200,000+ WordPress Sites to Takeover appeared first on SecurityWeek.

Zero-Day Flaw in TP-Link Cameras Enables Eavesdropping

Infosecurity Magazine - 16 September 2026 11:00

OPSWAT researchers find two zero-days in TP-Link cameras.

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-2026-58704 Google Pixel Improper Authorization Vulnerability.

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-2026-76460 Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability; CVE-2026-87886 Acronis Backup Incorrect Default Permissions Vulnerability

Threat actors and malware

Attackers Exploit Issabel Framework Flaw Enabling Unauthenticated OS Command Execution

The Hacker News - 16 September 2026 22:20

A critical security flaw in Issabel Framework, a web-based framework for the open-source unified communications PBX software, has come under active exploitation.

N0va Phishkit Targets US and EU Businesses: A New Challenge for Identity Security

The Hacker News - 16 September 2026 18:28

N0va is targeting organizations across North America and Europe with phishing campaigns that impersonate trusted services and abuse legitimate authentication flows. Successful attacks can give threat actors access to valid accounts without relying on obvious malware activity.

Google Patches Pixel Modem Flaw Amid Signs of Limited Targeted Exploitation

The Hacker News - 16 September 2026 17:45

Google has disclosed that a high-severity security flaw in its Pixel Cellular Modem has come under exploitation in the wild.The vulnerability, tracked as CVE-2026-58704 (CVSS score: 8.0), is a privilege escalation flaw.

Active Exploitation Triggers Emergency Patch for Cisco ISE Zero-Day

SecurityWeek - 17 September 2026 07:19

Remote, unauthenticated attackers can exploit the vulnerability to bypass authentication via crafted requests.The post Active Exploitation Triggers Emergency Patch for Cisco ISE Zero-Day appeared first on SecurityWeek.

Active Exploitation Attempts Target WSO2 API Manager JWT Bypass With Forged Admin Tokens

The Hacker News - 16 September 2026 11:48

Scottish Cyber Coordination Centre

A critical security flaw in WSO2 API Manager has come under active exploitation in the wild, according to findings from watchTowr.

Attackers Exploit WooCommerce Wholesale Lead Capture Flaw to Plant PHP Web Shells

The Hacker News - 16 September 2026 12:18

Threat actors are exploiting a critical security flaw in WooCommerce Wholesale Lead Capture, a premium WordPress plugin that has more than 6,000 active installs.

UK related

US, UK, Dutch Agencies Expose Iranian 'Chosen Brick' Surveillance Malware

SecurityWeek - 16 September 2026 13:00

US, UK, and Dutch government agencies published a report detailing the malware, and the FBI described the abuse of Telegram for C&C.The post US, UK, Dutch Agencies Expose Iranian 'Chosen Brick' Surveillance Malware appeared first on SecurityWeek.