



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

16 September 2026

Vulnerabilities

[CISA: Critical VMware RCE flaw now exploited by ransomware gangs](#)

BleepingComputer - 15 September 2026 09:16

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned security teams that ransomware gangs have now joined ongoing attacks exploiting a critical VMware vCenter vulnerability patched in July.

[Cisco Warns of Ongoing Exploitation of Critical Email Gateway Zero-Day](#)

Security Affairs - 15 September 2026 14:00

Cisco disclosed a critical zero-day, tracked as CVE-2026-76461 (CVSS score of 9.8), affecting Secure Email Gateway appliances. The flaw can be exploited remotely without authentication.

[Active Exploitation Attempts Target WSO2 API Manager JWT Bypass With Forged Admin Tokens](#)

The Hacker News - 16 September 2026 11:48

A critical security flaw in WSO2 API Manager has come under active exploitation in the wild, according to findings from watchTowr. The vulnerability, tracked as CVE-2026-5430 (CVSS score: 9.8/10.0), is a case of improper verification of a cryptographic signature that could result in account takeover.

[Acronis warns of actively exploited flaw in its cPanel backup plugin](#)

BleepingComputer - 15 September 2026 18:37

Acronis disclosed a high-severity Linux local privilege escalation vulnerability in its backup plugin for cPanel, WebHost Manager (WHM), and Plesk that may be exploited in the wild.

[One Exploit Chain, Two Espionage Campaigns: Chrome and Windows Under Fire](#)

Security Affairs - 15 September 2026 11:17

Two China-linked threat actors used the same Chrome/Windows zero-day against NGOs starting September 1, 2026, Volexity's new report lays out the whole chain in detail.

[Apple Patches 200 Vulnerabilities With New iOS 27, macOS Golden Gate 27 Releases](#)

SecurityWeek - 15 September 2026 12:06

The updates resolve kernel vulnerabilities that could lead to memory corruption, privilege escalation, system termination, and information leaks.



Scottish
Cyber
Coordination
Centre

Microsoft Releases Emergency Patch to Fix RDS Vulnerability

Infosecurity Magazine - 15 September 2026 09:40

Microsoft has been forced to issue an out-of-band fix for several issues stemming from this month's Patch Tuesday.

Threat actors and malware

KREMLIN Banking Malware Hijacks Chrome and Edge to Steal Credentials and Session Tokens

The Hacker News - 16 September 2026 01:24

Cybersecurity researchers have shed light on a previously undocumented Brazilian banking malware operation that delivers a toolkit called KREMLIN. Elastic Security Labs is tracking the activity under the moniker REF9334.

Iranian Hackers Use Telegram-Controlled Malware to Spy on Dissidents and Journalists

The Hacker News - 15 September 2026 22:59

Cybersecurity agencies in the United States, the United Kingdom, and the Netherlands have detailed a Windows malware that they say Iran's intelligence service uses to spy on dissidents, journalists, and activists around the world.

Mass-Scanning Campaign Exploits Vite Flaw to Extract Cloud Credentials From Exposed Dev Servers

The Hacker News - 15 September 2026 17:42

Cybersecurity researchers have disclosed details of a mass-scanning campaign that has targeted Vite deployments siphon sensitive data. The first is an automated effort aimed at internet-exposed Vite development servers that's designed to steal cloud credentials, configurations from Amazon Web Services (AWS) and Microsoft Azure instances, and infrastructure state files.