Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 August 2026

Vulnerabilities

Hackers exploit critical Adobe Commerce flaw to hijack customer accounts

Bleeping Computer - 12 August 2026 16:54

Attempts to exploit a critical vulnerability (CVE-2026-71362) in Adobe's Commerce and Magento e-commerce platforms have been detected, potentially allowing attackers to hijack customer accounts.

Lazarus hackers exploited Windows zero-day to target defense firms

Bleeping Computer - 12 August 2026 11:38

North Korean hackers have been exploiting a Windows zero-day vulnerability (CVE-2026-68820) to target defense-sector companies as part of the Operation Dream Job campaign.

Hackers leverage new Microsoft SharePoint exploit in attacks

Bleeping Computer - 12 August 2026 08:25

Hackers have already begun using a proof-of-concept (PoC) exploit for a critical Microsoft SharePoint vulnerability, published by cybersecurity company Rapid7 on Tuesday.

ShieldBreak: New Windows Zero-Day Bypasses Microsoft's RoguePlanet Patch

Security Affairs - 12 August 2026 08:07

Chaotic Eclipse released a PoC for ShieldBreak, a Microsoft Defender zero-day that bypasses the CVE-2026-50656 patch and could enable SYSTEM-level code execution.

Attackers Exploit VMware vCenter Vulnerability to Gain Persistent Remote Access

The Hacker News - 12 August 2026 14:31

Threat actors have begun to actively exploit a recently patched critical security flaw in Broadcom VMware vCenter, according to new findings from QUIRSO.The vulnerability in question is CVE-2026-59310 (CVSS score: 9.8), a directory-traversal vulnerability in the VMware vCenter server that a malicious actor with network access can exploit to execute arbitrary code.

Critical WordPress RCE Vulnerability Allows Authors to Execute Code via Malicious PNG File

Cyber Security News - 13 August 2026 02:36

WordPress has released version 7.0.4, a security-focused update that closes a remote code execution vulnerability affecting sites that process images with the Imagick extension and Ghostscript.

Scottish Cyber Coordination Centre

Google Chrome 151 Patches Five High-Severity Use-After-Free Flaws in V8, Blink, and Extensions

Cyber Security News - 12 August 2026 14:31

Google has officially released Chrome 151 to the Stable channel, mitigating five high-severity security vulnerabilities impacting key browser engine components, including the V8 JavaScript engine, Blink rendering engine, Chrome Extensions framework, HTML processing layer, and TabStrip.

Chipmaker Patch Tuesday: Intel, AMD Fix Over 80 Vulnerabilities Combined

Security Week - 12 August 2026 10:55

Intel has informed customers about several high-severity vulnerabilities that can lead to privilege escalation and even code execution.

Threat actors and malware

"City-Forum" data-theft attacks target Salesforce, ServiceNow portals

Bleeping Computer - 12 August 2026 19:07

An ongoing data theft campaign uses custom tools to steal data exposed to anonymous users through Salesforce Experience Cloud and ServiceNow customer portals.

WindRelay Malware Pairs With SpyNote RAT in Live-Call Scam

Infosecurity Magazine - 12 August 2026 14:30

New WindRelay NFC malware paired with SpyNote RAT let a fraudster clone a card mid-call.

Over 2,500 Organizations Impacted by LiteLLM Supply Chain Attack

Security Week - 12 August 2026 09:55

LiteLLM was compromised through the Trivy hack and abused to distribute information-stealing malware to its users.