Scottish Cyber Coordination Centre

Daily Threat Bulletin

14 August 2026

Vulnerabilities

SharePoint CVE-2026-55040 Comes Under Attack Following Public Exploit

Security Affairs - 13 August 2026 09:36

Attackers started exploiting CVE-2026-55040 (CVSS score of 9.1), a critical SharePoint authentication bypass patched in July, within days of Rapid7 releasing a public proof-of-concept on August 12.

Adobe Commerce CVE-2026-71362 Comes Under Attack Shortly After Public Disclosure

Security Affairs - 13 August 2026 18:48

Hackers began targeting a critical Adobe Commerce flaw that could let unauthenticated attackers hijack customer accounts and access private data. Hackers began targeting CVE-2026-71362 (CVSS score of 9.1), a critical Adobe Commerce flaw, shortly after its public disclosure.

Global Threat Campaign Hits Critical VMware vCenter Flaw

darkreading - 13 August 2026 21:45

Exploitation against CVE-2026–59310 began earlier this month, and patching the vulnerability may not be enough to fully mitigate the threat.

Microsoft patches LegacyHive Windows zero-day vulnerability

BleepingComputer - 13 August 2026 14:46

Microsoft has released security patches to address a Windows zero-day vulnerability known as “LegacyHive,” disclosed after the July 2026 Patch Tuesday.

WordPress 7.0.4 Patches Remote Code Execution Vulnerability

SecurityWeek - 13 August 2026 13:53

Attackers with Author-level user or higher permissions could exploit the flaw via malicious Postscript files.

Fortinet Patches Authentication Flaws in FortiWeb and FortiManager

SecurityWeek - 13 August 2026 11:40

The vulnerabilities could allow attackers to log in with random usernames and passwords or impersonate any FortiGate appliance.

Scottish Cyber Coordination Centre

Threat actors and malware

Akira hackers disable EDR with Safe Mode, steal data but fail to encrypt

BleepingComputer - 13 August 2026 17:47

An Akira ransomware affiliate disabled the endpoint detection and response (EDR) solution on a compromised system by restarting the machine into Safe Mode with Networking.

Storm-1175 Replaces Medusa With New StormEncryptor Ransomware

Security Affairs - 13 August 2026 09:09

Microsoft says China-linked Storm-1175 is using a new ransomware called StormEncryptor, replacing Medusa in its latest attacks. Microsoft says China-linked, financially motivated threat actor Storm-1175 has begun using a new ransomware strain called StormEncryptor.

North Korean Lazarus Group Uses Windows Zero-Day in Operation Dream Job

Security Affairs - 13 August 2026 08:05

Lazarus targets defense professionals with fake Lockheed Martin jobs, exploiting a Windows zero-day to deploy backdoors and evade security controls. Check Point Research has uncovered a new wave of Operation Dream Job, the long-running North Korean campaign that lures defense and aerospace professionals with convincing fake job offers.

AmnesiaStealer macOS Malware Steals Data, Controls Browser Sessions

SecurityWeek - 14 August 2026 07:41

The Rust-based macOS infostealer harvests users' passwords, keychain information, Chromium-based browser data, and Safari cookies.

#StopRansomware: Gunra Ransomware

CISA Advisories -

Gunra is a ransomware-as-a-service (RaaS) used by affiliates to target government, critical infrastructure, and other organizations. The Gunra ransomware variant first appeared in 2025 and expanded to RaaS operations in 2026.

UK Related

Exposed AWS Access Key Linked to Data Breach Affecting 1500+ UK Charities

Infosecurity Magazine - 13 August 2026 16:30

CRM provider Beacon has revealed that a compromised AWS access key was the likely root cause of the breach of 1500 UK charities' data.