Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 April 2026

Vulnerabilities

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-2026-35616 - Fortinet FortiClient EMS Improper Access Control Vulnerability. This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise.

Disgruntled researcher leaks “BlueHammer” Windows zero-day exploit

BleepingComputer - 06 April 2026 16:19

Exploit code has been released for an unpatched Windows privilege escalation flaw reported privately to Microsoft, allowing attackers to gain SYSTEM or elevated administrator permissions. [...]

Microsoft fixes Classic Outlook bug causing email delivery issues

BleepingComputer - 06 April 2026 16:19

Microsoft has resolved a known issue that was preventing some Classic Outlook users from sending emails via Outlook.com. [...]

Microsoft links Medusa ransomware affiliate to zero-day attacks

BleepingComputer - 06 April 2026 13:56

Microsoft says that Storm-1175, a China-based financially motivated cybercriminal group known for deploying Medusa ransomware payloads, has been deploying n-day and zero-day exploits in high-velocity attacks. [...]

Attackers Exploit RCE Flaw as 14,000 F5 BIG-IP APM Instances Remain Exposed

Security Affairs - 06 April 2026 14:07

Over 14,000 F5 BIG-IP APM instances remain exposed online, as attackers actively exploit a critical remote code execution flaw CVE-2025-53521. Over 14,000 F5 BIG-IP APM instances remain exposed online, with attackers actively exploiting the critical remote code execution vulnerability CVE-2025-53521 (CVSS ver. 3.1 score of 9.8), the nonprofit security organization Shadowserver warns.

Flowise AI Agent Builder Under Active CVSS 10.0 RCE Exploitation; 12,000+ Instances Exposed

The Hacker News - 07 April 2026 12:26

Scottish Cyber Coordination Centre

Threat actors are exploiting a maximum-severity security flaw in Flowise, an open-source artificial intelligence (AI) platform, according to new findings from VulnCheck.The vulnerability in question is CVE-2025-59528 (CVSS score: 10.0), a code injection vulnerability that could result in remote code execution.

Qilin and Warlock Ransomware Use Vulnerable Drivers to Disable 300+ EDR Tools

The Hacker News - 06 April 2026 16:37

Threat actors associated with Qilin and Warlock ransomware operations have been observed using the bring your own vulnerable driver (BYOVD) technique to silence security tools running on compromised hosts, according to findings from Cisco Talos and Trend Micro.

Automated Credential Harvesting Campaign Exploits React2Shell Flaw

darkreading - 06 April 2026 16:31

An emerging threat cluster tracked as UAT-10608 is exploiting vulnerable Web-exposed Next.js apps and using an automated tool to exfiltrate credentials, secrets, and other system data.

AppsFlyer SDK Exploited in New Supply Chain Crypto Attack

Security Boulevard - 07 April 2026 06:55

Between March 9 and March 11, 2026, attackers had a 48-hour window inside one of the most widely embedded JavaScript libraries on the internet.

AI agents found vulns in this popular Linux and Unix print server

The Register - 07 April 2026 00:03

CUPS server shown spilling out remote code execution and root access In the latest chapter on leaky CUPS, a security researcher and his band of bug-hunting agents have found two flaws that can be chained to allow an unauthenticated attacker to remotely execute code and achieve root file overwrite on the network....

Threat actors and malware

New GPUBreach attack enables system takeover via GPU rowhammer

BleepingComputer - 06 April 2026 18:44

A new attack, dubbed GPUBreach, can induce Rowhammer bit-flips on GPU GDDR6 memories to escalate privileges and lead to a full system compromise. [...]

BKA unmasks two REvil Ransomware operators behind 130+ German attacks

Security Affairs - 06 April 2026 15:48

German police BKA identified two key REvil ransomware members, linking them to over 130 attacks in Germany. Germany's Federal Criminal Police (BKA) has identified two key figures behind the REvil ransomware group, linking them to more than 130 attacks in the country. The first suspect is Daniil Maksimovich Shchukin (31), a Russian national known online [...]

Scottish Cyber Coordination Centre

AI-Assisted Supply Chain Attack Targets GitHub

darkreading - 06 April 2026 22:38

PRT-scan is the second in recent months where a threat actor appears to have leveraged AI for automated targeting of a widespread GitHub misconfiguration.

North Korean Hackers Target High-Profile Node.js Maintainers

SecurityWeek - 06 April 2026 12:02

The threat actor behind the Axios supply chain attack has been aiming at other maintainers in its social engineering campaign.