Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 April 2026

Vulnerabilities

Malicious PDF reveals active Adobe Reader zero-day in the wild

Security Affairs - 09 April 2026 20:14

Hackers used an Adobe Reader zero-day for months. Researcher Haifei Li found a malicious PDF and asks the community to help analyze it.

'BlueHammer' Windows Zero-Day Exploit Signals Microsoft Bug Disclosure Issues

darkreading - 09 April 2026 21:13

Under the alias 'Chaotic Eclipse,' a researcher released a PoC exploit for a zero-day flaw that allows for system takeover by a local user, citing an undisclosed beef with Microsoft.

Palo Alto Networks, SonicWall Patch High-Severity Vulnerabilities

SecurityWeek - 09 April 2026 12:58

The bugs could allow attackers to modify protected resources and escalate their privileges to administrator.

Threat actors and malware

New VENOM phishing attacks steal senior executives' Microsoft logins

BleepingComputer - 09 April 2026 18:37

Threat actors using a previously undocumented phishing-as-a-service (PhaaS) platform called "VENOM" are targeting credentials of C-suite executives across multiple industries.

Google Warns of New Threat Group Targeting BPOs and Helpdesks

Infosecurity Magazine - 09 April 2026 09:35

Google's threat intel team warns UNC6783, a new extortion group possibly linked to the "Raccoon" persona, is targeting BPOs and enterprises.

Masjesu botnet targets IoT devices while evading high-profile networks

Security Affairs - 09 April 2026 15:06

Masjesu is a stealthy DDoS-for-hire botnet targeting IoT devices, active since 2023 and designed to stay hidden by avoiding high-profile networks. It targets IoT devices like routers and gateways, spanning multiple architectures.

Scottish Cyber Coordination Centre

Chinese Supercomputer Allegedly Hacked, 10 Petabytes of Data Stolen

Security Magazine - 09 April 2026 16:00

Data has allegedly been stolen from a state-run Chinese supercomputer.