Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 July 2025

Vulnerabilities

Post SMTP plugin flaw exposes 200K WordPress sites to hijacking attacks

BleepingComputer - 26 July 2025 11:17

More than 200,000 WordPress websites are using a vulnerable version of the Post SMTP plugin that allows hackers to take control of the administrator account. [...]

Unpatched flaw in EoL LG LNV5110R cameras lets hackers gain Admin access

Security Affairs - 25 July 2025 21:39

Hundreds of LG LNV5110R cameras are affected by an unpatched auth bypass flaw that allows hackers to gain admin access. US Cybersecurity and Infrastructure Security Agency warns that hundreds of LG LNV5110R cameras are impacted by an unpatched authentication bypass vulnerability.

Mitel patches critical MiVoice MX-ONE Auth bypass flaw

Security Affairs - 25 July 2025 08:38

Mitel addressed a critical MiVoice MX-ONE flaw that could allow an unauthenticated attacker to conduct an authentication bypass attack. A critical authentication bypass flaw (CVSS score of 9.4) in Mitel MiVoice MX-ONE allows attackers to exploit weak access controls and gain unauthorized access to user or admin accounts.

Critical Flaws in Niagara Framework Threaten Smart Buildings and Industrial Systems Worldwide

The Hacker News - 28 July 2025 10:42

Cybersecurity researchers have discovered over a dozen security vulnerabilities impacting Tridium's Niagara Framework that could allow an attacker on the same network to compromise the system under certain circumstances.

Threat actors and malware

Scattered Spider is running a VMware ESXi hacking spree

BleepingComputer - 27 July 2025 12:05

Scattered Spider hackers have been aggressively targeting virtualized environments by attacking VMware ESXi hypervisors at U.S. companies in the retail, airline, transportation, and insurance sectors. [...]

Law enforcement operations seized BlackSuit ransomware gang's darknet sites

Scottish Cyber Coordination Centre

Security Affairs - 26 July 2025 14:48

An international law enforcement operation seized the dark web data leak site of the BlackSuit ransomware group. A banner on the BlackSuit ransomware group's TOR data leak sites informs visitors that they were seized by U.S. Homeland Security Investigations in a global law enforcement operation.

Operation CargoTalon targets Russia's aerospace with EAGLET malware,

Security Affairs - 25 July 2025 23:20

Operation CargoTalon targets Russia's aerospace and defense sectors with EAGLET malware, using TTN documents to exfiltrate data. SEQRITE Labs researchers uncovered a cyber-espionage campaign, dubbed Operation CargoTalon, targeting Russia's aerospace and defense sectors, specifically Voronezh Aircraft Production Association (VASO), via malicious TTN documents.

Overcoming Risks from Chinese GenAI Tool Usage

The Hacker News - 25 July 2025 16:55

A recent analysis of enterprise data suggests that generative AI tools developed in China are being used extensively by employees in the US and UK, often without oversight or approval from security teams.

Chinese Spies Target Networking and Virtualization Flaws to Breach Isolated Environments

SecurityWeek - 25 July 2025 10:22

Chinese cyberespionage group Fire Ant is targeting virtualization and networking infrastructure to access isolated environments.

UK related

UK Student Sentenced to Prison for Selling Phishing Kits

SecurityWeek - 25 July 2025 10:52

Ollie Holman was sentenced to prison for selling over 1,000 phishing kits that caused estimated losses of over $134 million.