Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 September 2025

Vulnerabilities

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2021-21311 Adminer Server-Side Request Forgery VulnerabilityCVE-2025-20352; Cisco IOS and IOS XE Stack-based Buffer Overflow Vulnerability; CVE-2025-10035 Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability; CVE-2025-59689 Libraesva Email Security Gateway Command Injection Vulnerability; CVE-2025-32463 Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability.

ForcedLeak flaw in Salesforce Agentforce exposes CRM data via Prompt Injection

Security Affairs - 27 September 2025 20:57

Researchers disclosed a critical flaw, named ForcedLeak, in Salesforce Agentforce that enables indirect prompt injection, risking CRM data exposure.

Increase in Scans for Palo Alto Global Protect Vulnerability (CVE-2024-3400), (Mon, Sep 29th)

SANS Internet Storm Centre - 29 September 2025 19:42

We are all aware of the abysmal state of security appliances, no matter their price tag. Ever so often, we see an increase in attacks against some of these vulnerabilities, trying to mop up systems missed in earlier exploit waves.

Threat actors and malware

Ransomware gang sought BBC reporter's help in hacking media giant

BleepingComputer - 29 September 2025 14:31

Threat actors claiming to represent the Medusa ransomware gang tempted a BBC correspondent to become an insider threat by offering a significant amount of money. [...]

Akira ransomware breaching MFA-protected SonicWall VPN accounts

BleepingComputer - 28 September 2025 15:49

Ongoing Akira ransomware attacks targeting SonicWall SSL VPN devices continue to evolve, with the threat actors found to be successfully logging in despite OTP MFA being enabled on accounts. Researchers suspect that this may be achieved through the use of previously stolen OTP seeds, although the exact method remains unconfirmed. [...]

Scottish Cyber Coordination Centre

Fake Microsoft Teams installers push Oyster malware via malvertising

BleepingComputer - 27 September 2025 16:49

Hackers have been spotted using SEO poisoning and search engine advertisements to promote fake Microsoft Teams installers that infect Windows devices with the Oyster backdoor, providing initial access to corporate networks. [...]

EvilAI Malware Masquerades as AI Tools to Infiltrate Global Organizations

The Hacker News - 29 September 2025 23:06

Threat actors have been observed using seemingly legitimate artificial intelligence (AI) tools and software to sneakily slip malware for future attacks on organizations worldwide.

UK related

UK govt backs JLR with £1.5 billion loan guarantee after cyberattack

BleepingComputer - 29 September 2025 13:31

The UK Government is providing Jaguar Land Rover (JLR) with a £1.5 billion loan guarantee to restore its supply chain after a catastrophic cyberattack forced the automaker to halt production. [...]

Cyberattack on Co-op leaves shelves empty, data stolen, and $275M in lost revenue

Security Affairs - 28 September 2025 17:25

The cyberattack on UK retailer Co-op in April caused empty shelves, customer data theft, and a $275M revenue loss. In May, the cybercrime group behind the April Co-op cyberattack, who go online with the name DragonForce, told the BBC that they had stolen data from the British retail and provided proof of the data breach. [...]

British Department Store Harrods Warns Customers That Some Personal Details Taken in Data Breach

SecurityWeek - 28 September 2025 19:07

Four people were arrested in July on suspicion of their involvement in cyberattacks against Harrods and two other leading British retail chains, Marks & Spencer and the Co-op and Harrods.

CISA and UK NCSC Release Joint Guidance for Securing OT Systems

CISA Advisories -

CISA, in collaboration with the Federal Bureau of Investigation, the United Kingdom's National Cyber Security Centre, and other international partners has released new joint cybersecurity guidance: Creating and Maintaining a Definitive View of Your Operational Technology (OT) Architecture.