Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 September 2026

Vulnerabilities

Nearly 22,000 Microsoft Exchange servers vulnerable to hijack attacks

Bleeping Computer - 01 September 2026 08:38

Nearly 22,000 Microsoft Exchange servers exposed online remain unpatched against a high-severity authentication bypass vulnerability that allows attackers to hijack all user mailboxes. [...]

Recently patched PaperCut zero-days used in data theft attacks

Bleeping Computer - 01 September 2026 03:48

Two security vulnerabilities in the PaperCut NG and MF print management software, patched last week after being exploited as zero-days, are now being abused in data theft attacks. [...]

Chaotic Eclipse Releases Kaspersky Zero-Day HardBreacher

Security Affairs - 01 September 2026 09:34

Chaotic Eclipse released HardBreacher, a PoC exploit for a Kaspersky Endpoint Security privilege escalation flaw, adding another zero-day to his list. Security researcher Chaotic Eclipse, also known as INFINITE NIGHTMARE, MSNightmare and Nightmare-Eclipse, released a new zero-day exploit targeting Kaspersky Endpoint Security.

Attackers Exploit Critical Langflow and Rails Flaws in Credential-Probing and C2 Activity

The Hacker News - 01 September 2026 12:52

Threat actors are exploiting two critical flaws impacting Langflow and Ruby on Rails, according to new findings from VulnCheck.The vulnerabilities in question are listed below - CVE-2026-0768 (CVSS score: 9.8) - A lack of proper validation of a user-supplied input vulnerability that could be exploited to execute arbitrary Python code in the context of the root user.

WatchGuard Patches Critical Vulnerabilities

Security Week - 01 September 2026 08:50

Three critical issues in the Fireware OS iked process could allow unauthenticated attackers to execute arbitrary code remotely.

JFrog Artifactory Auth Bypass Exploited in Attacks to Gain Admin Access

Cyber Security News - 01 September 2026 13:06

A critical authentication bypass vulnerability in JFrog Artifactory, tracked as CVE-2026-82329, is being actively exploited, allowing unauthenticated attackers with network access to gain administrator-level privileges. WatchTowr said its intelligence team has observed attackers exploiting the issue and “minting themselves admin tokens.”

Threat actors and malware

Hackers abuse Faronics Deploy admin tool to install ScreenConnect

Bleeping Computer - 01 September 2026 16:53

Phishing actors are abusing the legitimate Faronics Deploy endpoint-management platform to gain remote administrative control over victim computers and install the ScreenConnect remote support software. [...]

Hackers push malicious Virtualizor update in BGP hijacking attack

Bleeping Computer - 01 September 2026 10:45

Hackers delivered malicious updates to the Virtualizor VPS management software after hijacking BGP routing for its update infrastructure and redirecting update requests to malicious servers. [...]

Attackers Access Aesto Health AWS Infrastructure, Exposing 9.5 Million Records

Security Affairs - 01 September 2026 15:12

Aesto Health suffered a breach exposing personal and health data of more than 9.5 million people after attackers accessed its AWS infrastructure.

Iranian Hackers Pose as Recruiters to Deliver Cross-Platform RATs Through Coding Tests

The Hacker News - 01 September 2026 18:38

The Iranian Nimbus Manticore hacking group has been attributed to two previously undocumented malware families that highlight the continued evolution of its toolset and likely expand its targeting footprint to infect Linux and Apple macOS systems using cross-platform remote access trojans (RATs) developed using Node.js and JavaScript.

Attackers Steal METR API Key and Consume AI Credits Worth About $600,000

The Hacker News - 01 September 2026 14:35

METR (short for Model Evaluation and Threat Research and pronounced “Meter”), a research non-profit that evaluates frontier artificial intelligence (AI) models for their ability to carry out long-horizon, agentic tasks, disclosed that it suffered “two notable security incidents”.

Attackers Abuse Trusted Cloud Services to Hide Phishing Attacks Against Financial Organizations

Cyber Security News - 01 September 2026 15:04

Scottish Cyber Coordination Centre

Cybercriminals are increasingly weaponizing trusted cloud platforms such as Microsoft Azure, Google Firebase, Google Cloud Storage, Amazon Web Services, and Cloudflare to host phishing infrastructure aimed squarely at the financial sector, making malicious traffic nearly indistinguishable from legitimate business activity.

Hackers Pose as Recruiters and Send Fake Coding Tests to Infect Software Developers

Cyber Security News - 01 September 2026 13:40

Cybercriminals are posing as recruiters to turn routine job interviews into malware traps for software developers.

Hackers Weaponize Microsoft Teams Help Desk Calls for Malware and Network Lateral Movement

Cyber Security News - 01 September 2026 13:30

Attackers are turning Microsoft Teams help desk calls into an entry point for malware and network compromise.

Boston Scientific Cyberattack Disrupts Medical Device Manufacturing and Global Operations

Cyber Security News - 01 September 2026 13:15

Boston Scientific is investigating a cybersecurity incident that disrupted parts of its global operations, affecting manufacturing, order processing, and product shipments. The company said the incident was detected on August 25, 2026.