Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 September 2026

Vulnerabilities

New CrowdStrike 'FalconFlank' zero-day grants SYSTEM privileges

Bleeping Computer - 04 September 2026 09:22

An anonymous security researcher who uses the "Nightmare Eclipse" handle released a CrowdStrike Falcon zero-day exploit named "FalconFlank" that lets attackers escalate privileges on up-to-date Windows systems.

12-Year-Old PostgreSQL Vulnerability Enables Database, Server Takeover

Security Week - 04 September 2026 12:06

Dubbed PostGREShell, CVE-2026-6471 turns low-level replication access into code execution, permanent superuser privileges and a persistent database backdoor.

Sangoma Switchvox Vulnerabilities Exploited in the Wild

Security Week - 04 September 2026 13:23

Tracked as CVE-2026-9586, the unauthenticated SQL injection flaw can be exploited remotely for arbitrary code execution.

Elementor Pro WordPress Plugin Vulnerability Exploited to Hack Sites

Security Week - 05 September 2026 13:00

Tracked as CVE-2026-32475 (CVSS score of 9.8), the bug described as an arbitrary file upload issue in the function that handles form submissions.

Critical VMware Workstation and Fusion Flaw Lets VM Admins Execute Host Code

The Hacker News - 05 September 2026 21:35

Broadcom has released security updates for two security flaws impacting VMware Workstation and Fusion, including one critical bug that could result in arbitrary code execution under certain conditions.

ASUS Control Center Flaw Allows Attackers to Gain Full Admin Control of the System

Cyber Security News - 06 September 2026 10:57

ASUS has issued an urgent security update for ASUS Control Center Enterprise (ACC) after researchers uncovered a maximum-severity vulnerability that lets remote attackers seize complete administrative control over the platform and every device it manages, without needing a password or any user interaction.

Scottish Cyber Coordination Centre

N-able patches max severity N-central flaw amid ongoing attacks

Bleeping Computer - 07 September 2026 02:17

N-able has released an emergency hotfix for a maximum-severity remote code execution (RCE) flaw affecting its N-central remote monitoring and management (RMM) platform.

Threat actors and malware

Attackers conceal phishing lures using invisible Unicode characters

Bleeping Computer - 06 September 2026 10:23

Threat actors have adopted the ASCII smuggling technique in phishing campaigns, using invisible Unicode characters to evade email security filters.

Four REVSTEALER-Linked Modules Disable Windows Update and Defender to Run a Crypto Miner

The Hacker News - 06 September 2026 14:04

Elastic Security Labs has documented four previously unreported programs associated with REVSTEALER, an emerging Windows information stealer, that remain on an infected machine after the stealer deletes itself.One of them switches off Windows Update and Microsoft Defender before running a cryptocurrency miner.

Attackers Exploit PaperCut Flaws to Steal Credentials From Schools and Universities

The Hacker News - 05 September 2026 13:01

Threat actors are exploiting the newly disclosed PaperCut flaws to facilitate credential theft in attacks targeting the education sector in the U.S. and Europe.

Phishing Campaign Sends Millions of Emails Using Invisible Unicode to Evade Filters

The Hacker News - 04 September 2026 21:27

Microsoft is alerting of a “high-volume phishing campaign” that’s using invisible Unicode tag characters to bypass email filters.”

Hackers Exploiting MikroTik RouterOS Vulnerability in the Wild to Gain Complete Network Access

Cyber Security News - 06 September 2026 10:25

Attackers are actively exploiting an unauthenticated remote access flaw in MikroTik RouterOS, and network administrators worldwide are being urged to patch their devices immediately before compromise turns into a full network takeover.

UK related

Crooks Behind Manchester Airports Group Hack Leaked Data of 8.8 Million People

Security Affairs - 04 September 2026 18:30

Scottish Cyber Coordination Centre

Manchester Airports Group (MAG) data allegedly leaked by FulcrumSec exposes emails and phone numbers of 8.8 million people. Manchester Airports Group, which operates Manchester, London Stansted and East Midlands airports, has confirmed a data breach involving customer information held in a third-party database.