Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 September 2026

Vulnerabilities

CC-4840 - Exploitation of Zero-Day Vulnerabilities in SonicWall SMA1000 Series Appliances

NHS Digital - 02 September 2026 09:41

Severity: High Two zero-day vulnerabilities could be chained together to allow an unauthenticated attacker to perform RCE Two zero-day vulnerabilities could be chained together to allow an unauthenticated attacker to perform RCE.

WordPress backup plugin flaw exposes millions of sites to takeover attacks

Bleeping Computer - 02 September 2026 15:28

An SQL injection vulnerability in the All-in-One WP Migration and Backup plugin for WordPress could allow unauthenticated attackers to execute remote code and take control of affected websites.

SonicWall Patches Two New Actively Exploited Zero-Days in SMA 1000 VPNs

Security Affairs - 02 September 2026 14:22

SonicWall patched two zero-days in SMA 1000 VPNs, including a CVSS 10 pre-auth SSRF flaw, after confirming active exploitation. SonicWall has released security updates for two vulnerabilities in its SMA 1000 VPN appliances that are actively exploited in attacks in the wild.

Hackers Target Langflow in CVE-2026-0768 Attacks

Security Affairs - 02 September 2026 07:58

Hackers are exploiting a critical Langflow flaw that lets unauthenticated attackers remotely execute Python code on vulnerable systems. Hackers have started exploiting a critical vulnerability, tracked as CVE-2026-0768 (CVSS score of 9.8), in the AI-focused low-code platform Langflow.

CISA Adds Seven Known Exploited Vulnerabilities to Catalog

CISA - 02 September 2026 12:00

CISA has added seven new vulnerabilities to its catalog.

Researcher Claims CrowdStrike Falcon 0-Day Privilege Escalation Vulnerability

Cyber Security News - 03 September 2026 05:35

A security researcher known as Nightmare-Eclipse, who also goes by the names Chaotic Eclipse and MSNightmare, has released a project that claims to take advantage of a security flaw in the CrowdStrike Falcon Sensor.

Scottish Cyber Coordination Centre

Two critical Chrome flaws put users at risk on malicious websites

Malwarebytes - 02 September 2026 12:15

Update Chrome now: Two critical vulnerabilities could allow a malicious website to run code on your device.

Threat actors and malware

Hackers exploit Sangoma Switchvox flaw to deploy reverse shells

BleepingComputer - 02 September 2026 18:00

Attackers are actively exploiting CVE-2026-9586, an unauthenticated SQL injection vulnerability in the Sangoma Switchvox VoIP platform that can lead to remote code execution.

Hackers exploit critical JFrog Artifactory flaw to forge admin tokens

BleepingComputer - 02 September 2026 12:47

A critical authentication bypass vulnerability (CVE-2026-82329) in JFrog Artifactory is being exploited in attacks to create tokens that provide administrative access.

Attackers Exploit Critical Switchvox Flaw to Deploy Reverse Shells Without Credentials

The Hacker News - 02 September 2026 13:38

Threat actors are exploiting a severe security vulnerability in Sangoma Switchvox, an enterprise VoIP platform, that could allow unauthenticated remote code execution.

Authorities Turn Sality's P2P Network Against Itself, Cutting Off New Malware Payloads

The Hacker News - 02 September 2026 13:26

The U.S. Department of Justice (DoJ) on Tuesday announced the takedown of a long-standing peer-to-peer (P2P) botnet known as Sality as part of a coordinated law enforcement operation.

Threat Gang 'Springs' Vishing Attacks on Microsoft Teams Users

darkreading - 02 September 2026 17:51

The "Spring Ring" operation aims to compromise users of the collaboration suite to remotely access their sessions, spread malware, and even take over infrastructure.

Nutex Health Says Patient Data Stolen, Hackers Threaten Leak

Infosecurity Magazine - 02 September 2026 11:45

The US healthcare provider confirmed that sensitive patient and employee data, alongside financial and business information, were exfiltrated by a third party.

Scottish Cyber Coordination Centre

UK related

UK cyber bill targets AI users, not the vendors building it

The Register - 02 September 2026 11:44

Ministers reject proposed red lines and emergency shutdown powers, pointing instead to voluntary safeguards.