Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 September 2026

Vulnerabilities

CISA Warns of Multiple PaperCut NG/MF Vulnerabilities Actively Exploited in Attacks

Cyber Security News - 31 August 2026 16:56

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two vulnerabilities affecting PaperCut NG and PaperCut MF to its Known Exploited Vulnerabilities (KEV) Catalog, warning that threat actors are actively exploiting the flaws in real-world attacks. The flaws, addressing critical PaperCut vulnerabilities tracked as CVE-2026-81578 and CVE-2026-82078, can be chained to enable unauthenticated attackers [...]

D-Link Router Flaws Let Unauthenticated Attackers Change Admin Password and Steal Wi-Fi Credentials

Cyber Security News - 31 August 2026 16:44

D-Link has released a firmware update for critical access-control and information-disclosure flaws affecting its DIR-X1860Z router. The vulnerabilities could allow an unauthenticated attacker connected to the local network to change the router administrator password and recover wireless configuration details, including Wi-Fi credentials.

Critical GiveWP Flaw Lets Attackers Run Commands on WordPress Servers

Security Affairs - 31 August 2026 08:41

A critical GiveWP flaw lets unauthenticated attackers execute server commands. Version 4.16.7.2 fixes the PHP object injection chain. A critical vulnerability in GiveWP, one of the most widely used WordPress plugins for online donations and fundraising, can let an unauthenticated attacker execute commands on the server.

Nightmare Eclipse Drops 'HardBreacher' Kaspersky Product Exploit

SecurityWeek - 31 August 2026 15:32

Kaspersky told SecurityWeek that it patched the vulnerability affecting its Endpoint Security product.

ServiceNow Patches 3 Critical Code Injection Vulnerabilities

SecurityWeek - 31 August 2026 14:59

Attackers could exploit the security defects to execute arbitrary code and access or tamper with data.

Critical Ruby on Rails Vulnerability in Attackers' Crosshairs

SecurityWeek - 31 August 2026 12:24

Named KindaRails2Shell, the arbitrary file read flaw allows attackers to extract secrets and execute arbitrary code remotely.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-81578 PaperCut NG/MF Missing Authentication for Critical Function Vulnerability; CVE-2026-82078 PaperCut NG/MF Unsafe Reflection Vulnerability

Threat actors and malware

Hackers Target AWS Root Accounts at 150+ Organizations in Password-Spraying Campaign

Cyber Security News - 01 September 2026 07:07

Datadog Security Research observed a password-spraying campaign targeting AWS root accounts at more than 150 organizations between July 24 and August 23, 2026, with repeated failed console login attempts against highly privileged identities.

Hackers Hide ValleyRAT Backdoor Inside Adware Targeting Users in China and India

Cyber Security News - 31 August 2026 15:12

Hackers are using adware to deliver ValleyRAT, a Windows backdoor. The campaign primarily affects users in China and India, turning a program expected to display ads into a route for spying, theft, and further malware delivery.

Microsoft warns of TerminalFix attacks deploying reverse tunnels

BleepingComputer - 31 August 2026 15:51

A new ClickFix variant dubbed TerminalFix uses fake Cloudflare CAPTCHA prompts on compromised websites to trick victims into running malicious PowerShell commands in Windows Terminal. [...]

Chinese Fire Ant hackers turn Cisco routers into spying platforms

BleepingComputer - 31 August 2026 11:52

The researchers discovered Fire Ant's new tactic after finding an active GRE (Generic Routing Encapsulation) tunnel interface on a Cisco IOS XR router that could not be explained by a running configuration or commit history. [...]

Attack hides malware in PNGs and drops custom reverse tunnel on victims' machines

The Register - 31 August 2026 21:26

Next-level ClickFix wave sets off multi-stage attack chain