Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 November 2026

Vulnerabilities

CTM360 Exposes Fake Gift Card Scams Exploiting Trusted Brands

BleepingComputer - 07 November 2026 10:10

Scammers are impersonating major brands and celebrities to lure consumers into fake gift card giveaways that collect personal information and trigger unwanted subscriptions.

SonicWall warns of new SSL-VPN MFA bypass flaw exploited in attacks

BleepingComputer - 06 November 2026 20:00

SonicWall has released security updates to fix seven vulnerabilities in SonicOS firewalls, including an SSL-VPN authentication bypass flaw exploited in attacks. [...]

D-Link warns of multiple zero-days in DGS-3130 Series switches

BleepingComputer - 06 November 2026 08:37

D-Link shared mitigation measures for multiple unpatched security flaws affecting DGS-3130 series managed Gigabit stackable switches. [...]

Installing the Fix for an Exploited WordPress Flaw Can Expose Some Sites One Last Time

The Hacker News - 06 November 2026 22:38

Some WordPress sites can still be attacked while they install the fix for an actively exploited flaw, according to Umut Bayram, the Picus Security researcher who found it.

Hackers Target OpenSSH SSHole Flaw Within Hours of Disclosure, Gain Root on Honeypot

The Hacker News - 06 November 2026 21:51

Threat actors are attempting to exploit a recently disclosed security flaw impacting OpenSSH that can enable sign-ins to accounts that have no password set, according to Previdian.

Veeam Warns Critical 9.8 Linux Kernel Flaw Could Crash Backup Appliances and Disrupt Recovery Operations

Cyber Security News - 09 November 2026 08:48

Veeam warned that a critical Linux kernel flaw with a CVSS score of 9.8, could cause denial of service or memory corruption across backup and recovery products. Veeam's November 6 impact statement identified a Linux kernel use-after-free vulnerability (CVE-2026-98432) in TCP/IPv4 connection setup and outlined update paths for affected systems. Its security advisory does not [...]

Scottish Cyber Coordination Centre

Critical React Server Components Flaw Lets Hackers Execute Code Remotely Without Authentication

Cyber Security News - 09 November 2026 03:13

A critical security flaw in React Server Components can let attackers run code remotely without logging in. React published the advisory, tracked as GHSA-xqc2-xf4c-x3h3, on October 14, 2026.

OpenAI Says New GPT-6 Cyber Model Hunts Flaws Without Crossing the Line

SecurityWeek - 06 November 2026 14:19

Rated Critical for cybersecurity, OpenAI's new model beats GPT-5.6 Cyber at exploitation while staying in scope more reliably.

Threat actors and malware

Hackers pull off $133 million French bank heist via service provider

BleepingComputer - 07 November 2026 11:25

French cooperative bank Crédit Mutuel Arkéa was targeted in a cyberattack that enabled fraudulent transactions of up to $133 million, forcing it to respond by suspending certain systems.v [...]

Runaway AI hacking agent behind WorkOS breach after escaping sandbox

BleepingComputer - 06 November 2026 18:27

WorkOS says an AI-powered hacking agent that breached its internal sales application and accessed customer information was operated by a security researcher who claims the tool escaped its testing environment and unintentionally attacked the company. [...]

QNAP says hackers breaching NAS devices in Plex2Shell attacks

BleepingComputer - 06 November 2026 13:04

QNAP urges users to update Plex Media Server to the latest version available in the QNAP App Center, as hackers are exploiting the Plex2Shell vulnerability chain. [...]

U.S. Agencies Warn Refrigeration Controller Attacks Could Cause Fires and Inventory Losses

The Hacker News - 09 November 2026 12:45

U.S. government agencies have warned that threat actors are actively targeting industrial refrigeration and cold-chain monitoring systems globally with an aim to cause service disruptions, fire hazards, and loss of inventory.

Why Europe's Freezer Hacks Spread So Far, So Fast

darkreading - 06 November 2026 15:00

Scottish Cyber Coordination Centre

Europe's supermarket freezer hacks show how security issues can cascade across an industry, disrupting supply chains at scale.

UK related

UK Wades Into Tech Sovereignty Amid AI Policy Changes

darkreading - 06 November 2026 22:27

The UK is betting on domestic AI and cyber investment to reduce reliance on US tech — but security leaders question whether the funding is too fragmented and too late.

UK Warns Its Critical Infrastructure Faces Grave Risk

darkreading - 06 November 2026 10:00

Britain's new Labour-led government is making a concerted push to get ahead of the AI risks to its national networks and the industrial complex.