Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 November 2025

Vulnerabilities

Recent 7-Zip Vulnerability Exploited in Attacks

SecurityWeek - 20 November 2025 11:41

A proof-of-concept (PoC) exploit targeting the high-severity remote code execution (RCE) bug exists.

SolarWinds Patches Three Critical Serv-U Vulnerabilities

SecurityWeek - 20 November 2025 08:25

SolarWinds Serv-U is affected by vulnerabilities that can be exploited for remote code execution.

New SonicWall SonicOS flaw allows hackers to crash firewalls

BleepingComputer - 20 November 2025 11:56

American cybersecurity company SonicWall urged customers today to patch a high-severity SonicOS SSLVPN security flaw that can allow attackers to crash vulnerable firewalls.

D-Link warns of new RCE flaws in end-of-life DIR-878 routers

BleepingComputer - 20 November 2025 11:38

D-Link is warning of three remotely exploitable command execution vulnerabilities that affect all models and hardware revisions of its DIR-878 router, which has reached end-of-service but is still available in several markets.

Threat actors and malware

Google exposes BadAudio malware used in APT24 espionage campaigns

BleepingComputer - 20 November 2025 18:12

China-linked APT24 hackers have been using a previously undocumented malware called BadAudio in a three-year espionage campaign that recently switched to more sophisticated attack methods.

Sturnus: New Android banking trojan targets WhatsApp, Telegram, and Signal

Security Affairs - 20 November 2025 21:44

Sturnus is a new Android banking trojan with full device-takeover abilities. It bypasses encrypted messaging by capturing on-screen content and can steal banking credentials, remotely control the device, and hide fraudulent actions from the user.

Scottish Cyber Coordination Centre

TamperedChef Malware Spreads via Fake Software Installers in Ongoing Global Campaign

The Hacker News - 20 November 2025 10:36

Threat actors are leveraging bogus installers masquerading as popular software to trick users into installing malware as part of a global malvertising campaign dubbed TamperedChef. The end goal of the attacks is to establish persistence and deliver JavaScript malware that facilitates remote access and control.

CTM360 Exposes a Global WhatsApp Hijacking Campaign: HackOnChat

The Hacker News - 20 November 2025 18:00

CTM360 has identified a rapidly expanding WhatsApp account-hacking campaign targeting users worldwide via a network of deceptive authentication portals and impersonation pages. The campaign, internally dubbed HackOnChat, abuses WhatsApp's familiar web interface, using social engineering tactics to trick users into compromising their accounts.

US and Allies Sanction Russian Bulletproof Hosting Service Providers

SecurityWeek - 20 November 2025 13:53

Media Land, Hypercore, and their leadership and employees are allegedly connected to various cybercriminal activities.

Salesforce-linked data breach claims 200+ victims, has ShinyHunters' fingerprints all over it

The Register - 20 November 2025 21:30

They keep coming back for more Salesforce has disclosed another third-party breach in which criminals - likely ShinyHunters (again) - may have accessed hundreds of its customers' data.