Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 November 2025

Vulnerabilities

7-Zip RCE flaw (CVE-2025-11001) actively exploited in attacks in the wild

Security Affairs - 19 November 2025 20:23

A new 7-Zip flaw tracked as CVE-2025-11001 (CVSS score of 7.0) is now being actively exploited in the wild, NHS England warns. Remote attackers can trigger the vulnerability to execute arbitrary code on affected installations of 7-Zip.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2025-13223 Google Chromium V8 Type Confusion Vulnerability

W3 Total Cache WordPress plugin vulnerable to PHP command injection

BleepingComputer - 19 November 2025 13:34

A critical flaw in the W3 Total Cache (W3TC) WordPress plugin can be exploited to run PHP commands on the server by posting a comment that contains a malicious payload.

Threat actors and malware

New WrtHug campaign hijacks thousands of end-of-life ASUS routers

BleepingComputer - 19 November 2025 10:35

Thousands of ASUS WRT routers, mostly end-of-life or outdated devices, have been hijacked in a global campaign called Operation WrtHug that exploits six vulnerabilities.

Attackers are using “Sneaky 2FA” to create fake sign-in windows that look real

Malwarebytes - 19 November 2025 13:50

The Phishing-as-a-Service kit Sneaky 2FA was found to use Browser-in-the-Browser attacks to steal login credentials.

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.

Scottish Cyber Coordination Centre

US, UK, Australia sanction Lockbit gang's hosting provider

The Register - 20 November 2025 02:30

US, UK, Australia sanction Lockbit gang's hosting provider 'Bulletproof' hosts partly dodged the last attack of this sort Cybercrime fighters in the US, UK, and Australia have imposed sanctions on several Russia-linked entities they claim provide hosting services to ransomware gangs Lockbit, BlackSuit, and Play.

Meet ShinySp1d3r: New Ransomware-as-a-Service created by ShinyHunters

BleepingComputer - 19 November 2025 09:01

An in-development build of the upcoming ShinySp1d3r ransomware-as-a-service platform has surfaced, offering a preview of the upcoming extortion operation.

Half of Ransomware Access Due to Hijacked VPN Credentials

Infosecurity Magazine - 19 November 2025 10:40

Beazley Security data finds the top cause of initial access for ransomware in Q3 was compromised VPN credentials