Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

15 December 2025

Vulnerabilities

Apple fixes two zero-day flaws exploited in ‘sophisticated’ attacks

BleepingComputer - 12 December 2025 19:23

Apple has released emergency updates to patch two zero-day vulnerabilities that were exploited in an “extremely sophisticated attack” targeting specific individuals. […]

Notepad++ fixed updater bugs that allowed malicious update hijacking

Security Affairs - 12 December 2025 23:16

Notepad++ addressed an updater vulnerability that allows attackers hijack update traffic due to weak file authentication. Notepad++ addressed a flaw in its updater that allowed attackers to hijack update traffic due to improper authentication of update files in earlier versions.

U.S. CISA adds an OSGeo GeoServer flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 12 December 2025 10:24

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds an OSGeo GeoServer flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added an OSGeo GeoServer flaw, tracked as CVE-2025-58360 (CVSS Score of 8.2), to its Known Exploited Vulnerabilities (KEV) catalog.

CISA Adds Actively Exploited Sierra Wireless Router Flaw Enabling RCE Attacks

The Hacker News - 13 December 2025 19:03

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added a high-severity flaw impacting Sierra Wireless AirLink ALEOS routers to its Known Exploited Vulnerabilities (KEV) catalog, following reports of active exploitation in the wild.

New React RSC Vulnerabilities Enable DoS and Source Code Exposure

The Hacker News - 12 December 2025 15:25

The React team has released fixes for two new types of flaws in React Server Components (RSC) that, if successfully exploited, could result in denial-of-service (DoS) or source code exposure.

Gladinet CentreStack Flaw Exploited to Hack Organizations

SecurityWeek - 12 December 2025 14:49

Threat actors have hacked at least nine organizations by exploiting the recently patched Gladinet CentreStack flaw.

Threat actors and malware

Fake ‘One Battle After Another’ torrent hides malware in subtitles

BleepingComputer - 12 December 2025 13:12

A fake torrent for Leonardo DiCaprio’s ‘One Battle After Another’ hides malicious PowerShell malware loaders inside subtitle files that ultimately infect devices with the Agent Tesla RAT malware. [...]

Germany calls in Russian Ambassador over air traffic control hack claims

Security Affairs - 13 December 2025 19:14

Germany summoned Russia’s ambassador over alleged cyberattacks on air traffic control and a disinformation campaign ahead of national elections. Germany summoned Russia’s ambassador after accusing Moscow of cyber attacks against its air traffic control authority and running a disinformation campaign ahead of February’s election.

Elastic detects stealthy NANOREMOTE malware using Google Drive as C2

Security Affairs - 12 December 2025 12:11

Elastic found a new Windows backdoor, NANOREMOTE, similar to FINALDRAFT/REF7707, using the Google Drive API for C2. Elastic Security Labs researchers uncovered NANOREMOTE, a new Windows backdoor that uses the Google Drive API for C2.

VolkLocker Ransomware Exposed by Hard-Coded Master Key Allowing Free Decryption

The Hacker News - 15 December 2025 12:03

The pro-Russian hacktivist group known as CyberVolk (aka GLORIAMIST) has resurfaced with a new ransomware-as-a-service (RaaS) offering called VolkLocker that suffers from implementation lapses in test artifacts, allowing users to decrypt files without paying an extortion fee.

Fake OSINT and GPT Utility GitHub Repos Spread PyStoreRAT Malware Payloads

The Hacker News - 13 December 2025 01:20

Cybersecurity researchers are calling attention to a new campaign that’s leveraging GitHub-hosted Python repositories to distribute a previously undocumented JavaScript-based Remote Access Trojan (RAT) dubbed PyStoreRAT.

New Advanced Phishing Kits Use AI and MFA Bypass Tactics to Steal Credentials at Scale

The Hacker News - 12 December 2025 20:34

Cybersecurity researchers have documented four new phishing kits named BlackForce, GhostFrame, InboxPrime AI, and Spiderman that are capable of facilitating credential theft at scale.BlackForce, first detected in August 2025, is designed to steal credentials and perform

Man-in-the-Browser (MitB) attacks to capture one-time passwords (OTPs) and bypass multi-factor authentication (MFA). The kit

UK related

UK watchdog urged to probe GDPR failures in Home Office eVisa rollout

The Register - 12 December 2025 13:36

Rights groups say digital-only record is leaking data and courting trouble Civil society groups are urging the UK's data watchdog to investigate whether the Home Office's digital-only eVisa scheme is breaching GDPR, sounding the alarm about systemic data errors and design failures that are exposing sensitive personal information while leaving migrants unable to prove their lawful status....

NCSC Plugs Gap in Cyber-Deception Guidance

Infosecurity Magazine - 12 December 2025 11:30

The National Cyber Security Centre has released new learnings from a cyber deception pilot