Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 December 2025

Vulnerabilities

Hackers exploit newly patched Fortinet auth bypass flaws

BleepingComputer - 16 December 2025 11:57

Hackers are exploiting critical-severity vulnerabilities affecting multiple Fortinet products to get unauthorized access to admin accounts and steal system configuration files. [...]

React2Shell Vulnerability Actively Exploited to Deploy Linux Backdoors

The Hacker News - 16 December 2025 14:51

The security vulnerability known as React2Shell is being exploited by threat actors to deliver malware families like KSwapDoor and ZnDoor, according to findings from Palo Alto Networks Unit 42 and NTT Security.

Code Execution in Jupyter Notebook Exports

Security Boulevard - 16 December 2025 20:43

After our research on Cursor, in the context of developer-ecosystem security, we turn our attention to the Jupyter ecosystem. We expose security risks we identified in the notebook's export functionality, in the default Windows environment, to help organizations better protect their assets and networks.

JumpCloud Remote Assist Vulnerability Can Expose Systems to Takeover

SecurityWeek - 16 December 2025 12:39

The issue allows attackers to write arbitrary data to any file, or delete arbitrary files to obtain System privileges.

Threat actors and malware

Cellik Android malware builds malicious versions from Google Play apps

BleepingComputer - 16 December 2025 18:59

A new Android malware-as-a-service (MaaS) named Cellik is being advertised on underground cybercrime forums offering a robust set of capabilities that include the option to embed it in any app available on the Google Play Store. [...]

GhostPoster attacks hide malicious JavaScript in Firefox addon logos

BleepingComputer - 16 December 2025 18:17

Scottish Cyber Coordination Centre

A new campaign dubbed ‘GhostPoster’ is hiding JavaScript code in the image logo of malicious Firefox extensions counting more than 50,000 downloads, to monitor browser activity and plant a backdoor. […]

The Hidden Risk in Virtualization: Why Hypervisors are a Ransomware Magnet

BleepingComputer - 16 December 2025 11:01

Ransomware groups are targeting hypervisors to maximize impact, allowing a single breach to encrypt dozens of virtual machines at once. Drawing on real-world incident data, Huntress explains how attackers exploit visibility gaps at the hypervisor layer and outlines steps orgs can take to harden virtualization infrastructure. […]

Amazon Exposes Years-Long GRU Cyber Campaign Targeting Energy and Cloud Infrastructure

The Hacker News - 16 December 2025 18:57

Amazon’s threat intelligence team has disclosed details of a “years-long” Russian state-sponsored campaign that targeted Western critical infrastructure between 2021 and 2025.Targets of the campaign included energy sector organizations across Western nations, critical infrastructure providers in North America and Europe, and entities with cloud-hosted network infrastructure.

Venezuelan Oil Company Downplays Alleged US Cyberattack

darkreading - 16 December 2025 21:33

But media reports described the attack as causing major disruption to PDVSA, the state-owned oil and natural gas company.

Google Finds Five China-Nexus Groups Exploiting React2Shell Flaw

Security Boulevard - 16 December 2025 23:11

Researchers with Google Threat Intelligence Group have detected five China-nexus threat groups exploiting the maximum-security React2Shell security flaw to drop a number of malicious payloads, from backdoors to downloaders to tunnelers.