Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 December 2025

Vulnerabilities

Warning: WinRAR Vulnerability CVE-2025-6218 Under Active Attack by Multiple Threat Groups

The Hacker News - 10 December 2025 18:24

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a security flaw impacting the WinRAR file archiver and compression utility to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation. The vulnerability, tracked as CVE-2025-6218 (CVSS score: 7.8), is a path traversal bug that could enable code execution.

Fortinet fixed two critical authentication-bypass vulnerabilities

Security Affairs - 10 December 2025 23:04

Fortinet addressed 18 vulnerabilities, including two authentication-bypass flaws, tracked as CVE-2025-59718 and CVE-2025-59719 (CVSS score of 9.1), affecting FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager when FortiCloud SSO is enabled.

Microsoft Patch Tuesday security updates for December 2025 fixed an actively exploited zero-day

Security Affairs - 10 December 2025 09:47

Microsoft Patch Tuesday security updates for December 2025 addressed 57 vulnerabilities in Windows and Windows components, Office and Office Components, Microsoft Edge (Chromium-based), Exchange Server, Azure, Copilot, PowerShell, and Windows Defender.

SAP Patches Critical Vulnerabilities With December 2025 Security Updates

SecurityWeek - 10 December 2025 12:08

Affecting Solution Manager, Commerce Cloud, and jConnect SDK, the bugs could lead to code injection and remote code execution.

Ivanti EPM Update Patches Critical Remote Code Execution Flaw

SecurityWeek - 10 December 2025 12:53

The XSS vulnerability could allow remote attackers to execute arbitrary JavaScript code with administrator privileges.

Google Patches Gemini Enterprise Vulnerability Exposing Corporate Data

SecurityWeek - 10 December 2025 13:53

GeminiJack is a zero-click Gemini attack that could have been exploited using specially crafted emails, calendar invites, or documents.

Scottish Cyber Coordination Centre

Threat actors and malware

Active Attacks Exploit Gladinet's Hard-Coded Keys for Unauthorized Access and Code Execution

The Hacker News - 11 December 2025 12:26

Huntress is warning of a new actively exploited vulnerability in Gladinet's CentreStack and Triofox products stemming from the use of hard-coded cryptographic keys that have affected nine organizations so far.

New DroidLock malware locks Android devices and demands a ransom

BleepingComputer - 10 December 2025 17:53

A new Android malware called DroidLock has emerged with capabilities to lock screens for ransom payments, erase data, access text messages, call logs, contacts, and audio data.

ClickFix Style Attack Uses Grok, ChatGPT for Malware Delivery

darkreading - 10 December 2025 22:02

A new twist on the social engineering tactic is making waves, combining SEO poisoning and legitimate AI domains to install malware on victims' computers.

New EtherRAT backdoor surfaces in React2Shell attacks tied to North Korea

Security Affairs - 10 December 2025 15:45

North Korea–linked threat actors are likely exploiting the new critical React2Shell flaw (CVE-2025-55182) to deploy a previously unknown remote access trojan called EtherRAT, Sysdig researchers warn.

ClickFix Social Engineering Sparks Rise of CastleLoader Attacks

Infosecurity Magazine - 10 December 2025 17:45

A new malware campaign has been identified using a Python-based delivery system to deploy CastleLoader malware

New Spiderman phishing service targets dozens of European banks

BleepingComputer - 10 December 2025 10:53

A new phishing kit called Spiderman is being used to target customers of dozens of European banks and cryptocurrency holders with pixel-perfect cloned sites impersonating brands and organizations.