Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 June 2026

Vulnerabilities

Palo Alto GlobalProtect VPN auth bypass flaw now exploited in attacks

BleepingComputer - 30 May 2026 15:02

Palo Alto Networks is warning that hackers are now exploiting a PAN-OS GlobalProtect authentication bypass flaw, tracked as CVE-2026-0257, in attacks attempting to breach corporate networks. [...]

New CIFSwitch Linux flaw gives root on multiple distributions

BleepingComputer - 30 May 2026 11:16

A newly discovered local privilege escalation vulnerability dubbed 'CIFSwitch' in the Linux kernel could allow attackers to forge CIFS authentication key descriptions, abuse the kernel's key request mechanism, and gain root privileges. [...]

PAN-OS GlobalProtect Authentication Bypass (CVE-2026-0257) Under Active Exploitation

The Hacker News - 30 May 2026 13:11

Palo Alto Networks has warned that a recently disclosed medium-severity security flaw impacting PAN-OS and Prisma Access has come under active exploitation in the wild.The vulnerability, tracked as CVE-2026-0257 (CVSS score: 7.8), refers to a case of authentication bypass that could be exploited by bad actors to set up VPN connections..

ChatGPhish Vulnerability Turns ChatGPT Web Summaries Into a Phishing Surface

The Hacker News - 30 May 2026 00:37

Cybersecurity researchers have disclosed details of a vulnerability in OpenAI ChatGPT that leverages the artificial intelligence (AI) assistant's implicit trust in Markdown links and images to trigger prompt injections and open the door to phishing attacks. The technique has been codenamed ChatGPhish by Permiso Security.

Exploit Code Published for Critical Flowise RCE Vulnerability

SecurityWeek - 30 May 2026 16:55

The one-click vulnerability allows attackers to execute arbitrary code on self-hosted Flowise servers by tricking users into importing a malicious chatflow.

Gogs Zero-Day Exposes Servers to Remote Code Execution

SecurityWeek - 29 May 2026 13:59

The critical-severity issue, assigned a CVSS score of 9.4, is an argument injection flaw that can be exploited by authenticated attackers via pull requests with malicious branch names.

Chrome 148 Update Patches 151 Vulnerabilities

SecurityWeek - 29 May 2026 11:17

The browser update resolves critical-severity security defects that could potentially lead to remote code execution.

Threat actors and malware

ChatGPT share links abused to host fake outage pages to deliver malware

BleepingComputer - 29 May 2026 15:21

Threat actors are abusing ChatGPT's content-sharing feature to display fake OpenAI outage pages that direct users to download malware disguised as the ChatGPT desktop application. [...]

Attackers Use LLM Agent for Post-Exploitation After Marimo CVE-2026-39987 Exploit

The Hacker News - 29 May 2026 21:09

An unknown threat actor has been observed using a large language model (LLM) agent to conduct post-compromise actions after obtaining initial access following the exploitation of a publicly-accessible Marimo network using a recently disclosed vulnerability.

New Russia-Linked GREYVIBE Targets Ukraine with AI-Powered Cyberattacks

The Hacker News - 29 May 2026 18:01

A previously undocumented threat actor dubbed GREYVIBE has been attributed to ongoing and persistent attacks targeting Ukraine and Ukraine-related entities since at least August 2025.

Malicious Sicoob NuGet Steals Banking Credentials as npm Packages Target Cloud Secrets

The Hacker News - 29 May 2026 15:41

Cybersecurity researchers have discovered a malicious NuGet package that masquerades as a C# software development kit for Sicoob, one of Brazil's largest cooperative financial systems, to siphon client IDs and PFX certificates.

What To Do When You're Under a DDoS Attack

Security Boulevard - 31 May 2026 06:42

DDoS protection gaps usually become visible when there is the least room to investigate them: during an active attack. Traffic volumes rise, services begin to degrade, and the response team has to determine whether the issue is attack volume, routing, mitigation coverage, application-layer bypass, or an exposed asset that was never protected in the first [...]

Scottish Cyber Coordination Centre

UK related

Backup and recovery architecture best practices for UK SMEs

Security Boulevard - 31 May 2026 06:28

Backup and recovery architecture best practices for UK SMEs For many UK SMEs, backup is treated as a storage task. In practice, it is a business resilience control. A good backup and recovery design helps you keep trading after accidental deletion, system failure, cyber attack, or a supplier outage. It also reduces the pressure on [...]The post Backup and recovery architecture best practices for UK SMEs appeared first on Clear Path Security Ltd.