Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 May 2026

Vulnerabilities

Microsoft SharePoint Has a New RCE Flaw. If You Haven't Patched Yet, Go Do That.

Security Affairs - 27 May 2026 08:10

A critical vulnerability, tracked as CVE-2026-45659, in Microsoft SharePoint can allow attackers to achieve remote code execution with little effort.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-8398 Daemon Tools Lite Embedded Malicious Code Vulnerability

CVE-2026-45321 TanStack Unspecified Vulnerability

CVE-2026-48027 Nx Console Embedded Malicious Code Vulnerability

Gitea Vulnerability Exposes Private Container Images without Authentication

The Hacker News - 27 May 2026 16:36

Cybersecurity researchers have disclosed a security flaw in Gitea, an open-source, self-hosted platform for version control, that allows unauthenticated remote attackers to pull private container images from Gitea deployments without requiring an account, password, or other credentials.

AI-Assisted Exploit Development Outpaces Scanner Detection

darkreading - 27 May 2026 17:11

Attackers are using AI to dramatically reduce the time they need to develop a working exploit for a CVE, according to new research.

Vulnerability in Popular Conference Software Granted Attackers a 100% Talk Acceptance Rate

SecurityWeek - 27 May 2026 15:30

Novee researchers discovered an account takeover vulnerability in the open source CFP management tool Pretalx.

Scottish Cyber Coordination Centre

Threat actors and malware

Grandoreiro Malware and BTMOB RAT Campaigns Target Windows and Android Users

The Hacker News - 27 May 2026 22:40

Latin America and Europe become the target of two banking trojan campaigns that are designed to infect Windows and Android devices with Grandoreiro and BTMOB malware, respectively.

UK Cyberspying Chief Calls AI 'an Unstoppable Force' and Warns About Russia

SecurityWeek - 27 May 2026 18:32

The speech is the latest in a string of warnings from intelligence experts that Russia is stepping up hostile activity in a "gray zone" that falls just below the threshold of war.

GlassWorm Malware Takedown Disrupts Developer Supply Chain Attack Infrastructure

The Hacker News - 27 May 2026 18:18

CrowdStrike, in partnership with Google and the Shadowserver Foundation, has announced the simultaneous disruption of all command-and-control (C2) channels associated with GlassWorm, a persistent software chain campaign targeting software developers through malicious packages and extensions.

GPU mining malware spreads via SEO poisoning, AI chatbots

BleepingComputer - 27 May 2026 18:31

Threat actors are targeting systems with high-performance computers in an ongoing cryptojacking campaign spread through a coordinated SEO poisoning operation that also manipulated AI chatbot recommendations.

Thousands of Fake FIFA Domains Target World Cup Fans

Infosecurity Magazine - 27 May 2026 12:28

Group-IB uncovered Ghost Stadium phishing and 4300 fake FIFA World Cup domains targeting fans.