Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 November 2026

Vulnerabilities

Over 1,000 GitLab servers vulnerable to ongoing RCE attacks

BleepingComputer - 02 November 2026 08:47

Over 1,000 Internet-exposed GitLab servers are still unpatched against a maximum-severity flaw actively exploited in remote code execution attacks. [...]

Critical Langflow Flaws Could Let Unauthenticated Attackers Run Code on Servers

The Hacker News - 02 November 2026 18:20

Two critical flaws in Langflow could let a remote attacker with no account bypass authentication or run arbitrary code, IBM said last week.Langflow is an open-source tool for building AI agents and workflows, and its vulnerability reports go to IBM.

OpenAI Launches New Security Sprint to Hunt Vulnerabilities and Strengthen Defenses

Cyber Security News - 03 November 2026 06:17

OpenAI is preparing a new internal security sprint that will bring outside researchers together with its own teams to find vulnerabilities, test fixes, and strengthen its platforms using AI.

Max-severity bug in widely used OT programming tool exploited to deliver Linux malware

The Register - 03 November 2026 00:55

Your industrial IoT gateway isn't exposed to the internet, right? RIGHT?!

Ivanti Patches Two More Zero-Days Exploited in Connect Secure Attack Chain

SecurityWeek - 02 November 2026 08:57

CISA has added CVE-2026-111357 and CVE-2026-118527 to its KEV catalog after the Ivanti VPN flaws were chained in zero-day attacks.

Threat actors and malware

Google disrupts million-device XCPE Android malware botnet, bans TV box maker

BleepingComputer - 02 November 2026 14:16

Google and industry partners have dismantled the XCPE malware botnet consisting of more than 1.3 million Android TV streaming TV boxes that Google says its manufacturer intentionally infected with malware to generate revenue through cybercrime activities. [...]

Scottish Cyber Coordination Centre

Attackers Exploit Critical Siemens IoT2050 Flaw to Plant Remote Command Backdoors

The Hacker News - 03 November 2026 12:04

A maximum-severity security flaw impacting Siemens SIMATIC IoT2050 Advanced devices has come under active exploitation, VulnCheck has revealed.The vulnerability, tracked as CVE-2026-58115 (CVSS score: 10.0), is a case of missing authentication for a critical function that could be exploited by an unauthenticated remote attacker to run arbitrary code.

Attackers Pose as IT Support on Microsoft Teams, Abuse AD CS to Steal Company Data

The Hacker News - 02 November 2026 17:38

Attackers posing as IT support on Microsoft Teams talked employees into giving them remote control of their PCs. They then used insecure Active Directory Certificate Services (AD CS) settings to obtain login certificates for privileged accounts, including one for a domain controller.

Government Linux Servers Targeted With SysGoRAT and Suspected AI-Generated Scripts

The Hacker News - 02 November 2026 17:19

Cybersecurity researchers have disclosed details of a cyber espionage campaign specifically targeting Linux infrastructure associated with government entities and state-affiliated infrastructure.T

Hackers Use Malicious VHDX Files and WebDAV Links to Infect Windows Devices With PapRAT Malware

Cyber Security News - 03 November 2026 07:44

A suspected espionage group is sending fake meeting letters and event invitations to organizations in South Asia. The files look harmless, but they quietly install a custom remote access trojan called PapRAT on Windows computers. The campaign uses Windows disk images, shortcut files, and remote web folders to avoid easy detection.

Hackers Use ARTEX AI to Breach WorkOS and Access Customer Slack Conversations

Cyber Security News - 03 November 2026 04:43

WorkOS has confirmed unauthorized access to an internal sales application, exposing customer contact information and records of business conversations. The company detected the incident on October 30, 2026, and published a security bulletin on November 2.

New wave of fridge cyberattacks hits European supermarkets, this time in Belgium, Luxembourg, Sweden and Estonia

Security Affairs - 02 November 2026 13:09

A new wave of fridge cyberattacks hit supermarket refrigeration systems across five European countries, raising temperatures and causing food losses. A new wave of fridge cyberattacks

has affected supermarket refrigeration systems in several European countries. Fridges and freezers suddenly rose in temperature overnight, with some incidents suspected to be caused by hackers. On Monday, November [...]

UK related

Cyber chief: UK facing AI-powered attacks on critical infrastructure within two years

NCSC - 03 November 2026 13:00

The NCSC warns that 'tech on the cheap' has left UK organisations exposed to AI uncovering and exploiting longstanding cyber security weaknesses and calls for urgent investment in resilience.

Artificial intelligence and cyber intrusion

NCSC - 03 November 2026 13:00

An NCSC assessment that examines current AI-enabled threat trends and projections of the threat landscape to 2028.