Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 November 2026

Vulnerabilities

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.CVE-2026-114713 UnrealIRCd Improper Neutralization of Delimiters VulnerabilityCVE-2026-123039 Check Point Multiple Products Incorrect Permission Assignment for Critical Resource Vulnerability

Researchers continue to find serious vulnerabilities in internet connected refrigerators

CyberScoop - 13 November 2026 22:20

VulnCheck disclosed 14 vulnerabilities in Dixell refrigeration units that give an attacker root access, while online honeypots are being flooded with hacks and malicious probes.

PostgreSQL Patches 52 Flaws, Including 22-Year-Old Bug Enabling Authenticated RCE

The Hacker News - 13 November 2026 23:23

A type confusion flaw in PostgreSQL lets a database user who can create objects run code on the server. Updates released yesterday fix it, along with 51 other security flaws. Full protection from this flaw also requires rebuilding any C-language extensions installed on the server.The flaw, tracked as CVE-2026-6460, has a CVSS score of 8.8.

NoisyTCP: 11-Year-Old Linux Kernel Flaw Lets Unauthenticated Attackers Crash Servers Remotely

Cyber Security News - 16 November 2026 06:26

NoisyTCP is an 11-year-old Linux kernel bug. It lets a remote attacker crash a server without logging in. The flaw is tracked as CVE-2026-99288. Hyunwoo Kim (@v4bel) reported and patched it, and he released the NoisyTCP advisory on GitHub after the Linux distribution embargo ended. The flaw sits in the kernel's TCP code, which handles [...]

Threat actors and malware

FBI warns ARTEX AI hacking tool is powering global cyberattacks

BleepingComputer - 15 November 2026 14:29

The FBI is warning that hackers are using an AI-powered penetration testing framework called ARTEX to automate cyberattacks against organizations worldwide, including a recent

ConnectWise supply-chain breach that compromised Microsoft 365 customer environments. [...]

Check Point gateways hacked via PHP2Shell to deploy VMware ESXi wiper

BleepingComputer - 13 November 2026 12:21

Vulnerable Check Point Security Gateway instances have been targeted in PHP2Shell attacks that deployed data-wiping malware on VMware ESXi hosts. [...]

Amazon Uncovers AI Agent Campaign Targeting LiteLLM, Dify, and Other Apps for API Keys

The Hacker News - 16 November 2026 14:04

Attackers' AI agents have been hunting for weak spots in internet-exposed AI apps such as LiteLLM, One API, and Dify to steal the AI provider keys stored inside, according to the agents' own records.The records, which Amazon's threat intelligence team captured with decoy servers, describe stolen keys being used to run the AI models that powered the search for more keys.

BO Team Exploits Log4Shell in VMware vCenter, Compromises Russian Firm's Code-Signing Server

The Hacker News - 16 November 2026 13:23

An investigation into suspicious activity within a Russian software developer's network has uncovered a months-long compromise of its development infrastructure and a software code-signing server.

New Mior and Skyfall Attacks Let Rogue Cloud Hosts Steal Secrets From AMD SEV-SNP VMs

The Hacker News - 13 November 2026 21:57

Two attacks made public this week allow a malicious host to read data inside AMD SEV-SNP-protected virtual machines (VMs), which are built to keep the server's operator out.

Hackers Exploit N-central Flaws to Infect 21 Servers, Including 19 Running Hotfix 2

The Hacker News - 13 November 2026 12:13

N-able on Thursday said it's taking additional precautions in the wake of public disclosure of a new set of flaws tracked as 4EverAble2Shell and Agent2Shell."We are restricting certain N-central features and integrations," the company said in a Thursday update. "