Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 November 2026

Vulnerabilities

Google Project Zero cuts bug disclosures to 30 days amid AI threats

BleepingComputer - 16 November 2026 17:31

Google Project Zero will replace its “90+30” disclosure policy with shorter, fixed deadlines in response to AI-accelerated vulnerability discovery and exploitation. […]

Microsoft says months-old bug caused global Microsoft 365 outage

BleepingComputer - 16 November 2026 12:43

Microsoft says a software bug introduced in July caused last week’s worldwide Microsoft 365 outage, triggering a cascading failure that left more than 80% of its networking gateway servers unresponsive. […]

N-able Patches 17 N-central Flaws as Attackers Exploit Earlier Bugs to Deploy Crypto Miners

The Hacker News - 17 November 2026 11:30

N-able has released a new security update to address additional critical security flaws impacting N-central.Describing N-central 2026.4 Hotfix 3 as a critical security update, the company said it includes a number of security patches and fixes that enhance the security of the Remote Monitoring and Management (RMM) and Unified Endpoint Management (UEM) platform.”

Six Unpatched Danfoss Refrigeration Controller Flaws Could Allow Remote Takeover Without Login

The Hacker News - 16 November 2026 19:04

Six flaws in Danfoss AK-SM800A refrigeration controllers could let a remote attacker take over a controller without logging in, Dutch security consultancy Midnight Blue said earlier this week.No patch is available, and the researchers say the newest firmware, version 5.4.0, does not fix the flaws.

Chase Software Bug Disrupts Banking Services as Customers Report Outages at Major US Banks

Cyber Security News - 17 November 2026 04:05

A software bug at JPMorgan Chase disrupted banking services on November 16, 2026, leaving thousands of customers reporting trouble with account access and payments. Complaints also appeared for Bank of America, Wells Fargo, U.S. Bank and Zelle, though reports did not establish separate outages at each bank. Chase linked the disruption to a temporary software […]

Scottish Cyber Coordination Centre

Recent UnrealIRCd Vulnerability Exploited in Attacks

SecurityWeek - 16 November 2026 12:15

Tracked as CVE-2026-114713, the high-severity flaw allows attackers to execute commands with server/IRCOp privileges.The post Recent UnrealIRCd Vulnerability Exploited in Attacks appeared first on SecurityWeek.

Threat actors and malware

Google says Russian-speaking hackers ran the first fully automated AI cyberattack

CyberScoop - 16 November 2026 23:51

Google's Threat Intelligence Group says the tools trade stealth for speed, leaving noisy forensic traces even as they succeed on their own.

Gemini AI agents repeatedly bypassed safeguards to attack real website

BleepingComputer - 16 November 2026 18:54

Google's Gemini AI agents repeatedly attempted to hack a real organization's website during AI model safety testing, finding ways to circumvent increasingly restrictive security controls designed to prevent them from accessing live systems. [...]

Barracuda links cloud breach to ARTEX AI-powered cyberattack

BleepingComputer - 16 November 2026 15:57

Hackers who breached the cloud environment of network and email security company Barracuda earlier this month used a stolen cloud access key and the ARTEX AI penetration testing framework. [...]

Retadup Worm Resurfaces 7 Years After Takedown to Spread CoffeeLoader Malware

The Hacker News - 16 November 2026 19:03

Cybersecurity researchers have disclosed details of a new variant of CoffeeLoader, a malware designed to deliver additional payloads to infected machines."On launch, the NSIS-based installer executable dropped a file named '7z.dll' into a temporary directory and ran it through rundll32.exe," Kaspersky said in an analysis published today.

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.

Cisco Talos Reveals How Hackers Use ARTEX, PentAGI, and HexStrike AI to Automate Cyberattacks

Scottish Cyber Coordination Centre

Cyber Security News - 16 November 2026 16:48

AI-powered penetration testing tools are helping hackers automate reconnaissance, vulnerability testing, and follow-on attacks with less hands-on work. Cisco Talos warns that these platforms can connect familiar security utilities with AI agents, allowing operators to pursue targets faster and run several tasks at once. The danger comes from how legitimate testing capabilities are being used [...]