Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 November 2026

Vulnerabilities

Microsoft scrambles to solve global outage affecting tens of thousands

BBC News – 13 November 2026

A Microsoft outage is continuing to affect users in at least 74 countries around the world - Services including Teams, Outlook and AI software Copilot have been hit with connectivity problems for more than 10 hours.

New N-able "4EverAble2Shell" zero-day exploited hours after PoC released

BleepingComputer - 12 November 2026 15:51

Hackers are actively exploiting a newly disclosed N-able N-central zero-day vulnerability dubbed "4EverAble2Shell" to compromise servers and deploy cryptocurrency miners, with researchers reporting at least 21 affected systems, including 19 running the company's latest security update.

Apache HTTP Server patches critical HTTP/2 remote code execution flaw

BleepingComputer - 12 November 2026 15:12

A critical vulnerability in the HTTP/2 module of Apache HTTP Server could be exploited by an unauthenticated attacker to obtain remote code execution (RCE).

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.

Zoom Fixes Critical Windows Vulnerability Allowing Privilege Escalation

Security Affairs - 12 November 2026 13:33

Zoom fixes two Windows Workplace flaws, including a critical bug that could let unauthenticated attackers remotely escalate privileges.

Critical Red Hat Quay Vulnerability Could Expose Private Container Images

SecurityWeek - 12 November 2026 10:23

Attackers could exploit a critical Red Hat Quay flaw to steal private container images, overwrite repositories and maintain persistent access.

Scottish Cyber Coordination Centre

Google Cloud Warns Three AMD Turin CPU Flaws Could Leak Data Across Processes in VMs

The Hacker News - 12 November 2026 18:39

Google Cloud VMs on AMD Turin chips need a guest OS patch and a stop-and-start to protect against three CPU side-channel flaws, Google said this week. The company has already applied mitigations against attacks between VMs, and between VMs and the host.

Citrix Patches 12 NetScaler and Secure Access Client Flaws, Including Authentication Bypass

The Hacker News - 12 November 2026 22:08

Citrix has released patches for multiple critical security flaws impacting NetScaler ADC, Citrix NetScaler Gateway, and NetScaler Console that could lead to denial-of-service (DoS) or an authentication bypass.

Chrome, Firefox Updates Patch Over 180 Vulnerabilities

SecurityWeek - 12 November 2026 14:42

Google fixed 83 flaws with a new Chrome 157 release, and Mozilla addressed 99 bugs in Firefox 160.

Node.js Fixes 16 Flaws, Including HTTP/2 Bugs That Crash Servers and Leak Other Connections' Data

The Hacker News - 12 November 2026 14:50

A flaw fixed in Node.js this week lets unauthenticated clients crash servers that use the runtime's built-in HTTP/2 support on the 24.x and 26.x release lines. A second HTTP/2 flaw can cause a server to send a client pieces of its memory, including responses intended for other connections.

Threat actors and malware

New worm-like 'SCKit' malware targets MSPs in ScreenConnect attacks

BleepingComputer - 12 November 2026 18:53

A new worm-like malware toolkit named SCKit was deployed in the recent ScreenConnect attacks targeting managed service providers (MSPs), designed to spread from infected customer devices to MSP technicians' computers and compromise additional managed networks.

Attacker Used 4,837 Hijacked GitHub Accounts to Run a CI Secret Stealer in 1,806+ Repositories

The Hacker News - 12 November 2026 13:12

Starting Tuesday, an attacker used stolen credentials for 4,837 GitHub accounts to plant a secret stealer in repositories those accounts could write to, according to Aikido Security, a security software company.

Scottish Cyber Coordination Centre

186 Fake AI Domains Redirect Users to ClickFix Lures, Browser Malware, and Search Hijackers

The Hacker News - 12 November 2026 21:45

Cybersecurity researchers have found that lookalike domains masquerading as artificial intelligence (AI) tools are being used to serve ClickFix-style lures, browser-hijacking malware, and a set of extensions that hijack user searches.

Apify rotates API tokens, prompts 2FA resets after breach

BleepingComputer - 12 November 2026 10:36

Apify has rotated critical internal secrets and revoked some third-party OAuth connections after detecting unauthorized access to its internal systems.

Police dismantle Gootloader, CastleRAT, StealC malware infrastructure

BleepingComputer - 12 November 2026 11:07

Europol and law enforcement partners from nine countries have seized hundreds of servers and domains used by the Gootloader, CastleRAT, and StealC malware operations.

UK incidents

The School Bomb Threats Came From Accounts Already in Stolen Data

Security Affairs - 12 November 2026 23:42

Hudson Rock researchers found that two university addresses tied to Italy's school bomb threats were in infostealer data. On 11 November, bomb-threat emails hit schools across Europe. ANSA, citing the Education Ministry, reported that about 6,000 Italian schools received them.