Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 November 2026

Vulnerabilities

Attackers Chain Three Ivanti Connect Secure Flaws to Gain Unauthenticated Root Access

The Hacker News - 31 October 2026 14:57

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added two security flaws impacting Ivanti Connect Secure (ICS) to its Known Exploited Vulnerabilities (KEV) catalog, following active exploitation in the wild.

Attackers Exploit Critical Drupal Commerce Core Vulnerability CVE-2026-118539

Security Affairs - 31 October 2026 10:08

Drupal warns that attackers are exploiting a critical authorization flaw in Commerce Core, putting vulnerable online stores at risk.

WordPress RCE Flaw Draws Nearly 63,000 Attack Attempts in Just 24 Hours

The Hacker News - 30 October 2026 20:38

Threat actors have been observed attempting to exploit a high-severity security flaw in WordPress Core shortly after patches were released. The vulnerability, which does not have a CVE identifier, relates to a case of remote code execution impacting WordPress Core versions 4.7 through 7.1.3.

Max-Severity GitLab Vulnerability Exploited Against Alpine Linux

SecurityWeek - 30 October 2026 10:32

Tracked as CVE-2026-97229, the bug allows unauthenticated attackers to execute arbitrary code on the server.

New Android SMS of Death exploit can remotely crash unpatched phones

BleepingComputer - 31 October 2026 12:35

A security researcher has released a proof-of-concept exploit for a recently patched Android vulnerability, dubbed “SMS of Death” and tracked as CVE-2026-58882, that lets attackers remotely disrupt cellular service or crash phones by sending a specially crafted text message.

Critical Linux kernel flaw allows remote root attacks on MPTCP servers

BleepingComputer - 30 October 2026 18:09

Security researchers at Anthropic have developed an exploit for a critical Linux kernel vulnerability that allows unauthenticated attackers to remotely execute commands as root on servers running Multipath TCP (MPTCP) listeners.

Scottish Cyber Coordination Centre

TeamViewer Flaw Lets Remote Computers Attack Users Who Connect to Control Them

The Hacker News - 30 October 2026 21:47

TeamViewer has fixed a flaw that lets the machine being controlled in a remote session attack the computer that connected to control it.

Threat actors and malware

NetamLoader Malware Targets Government Windows 10 Systems in Asia via .NET Injection

The Hacker News - 01 November 2026 13:32

Cybersecurity researchers have disclosed details of what has been described as a “highly sophisticated infection chain” targeting government organizations in Asia.

Northflank security breach leads to abuse of customers’ AI API keys

BleepingComputer - 31 October 2026 15:01

Cloud application hosting platform Northflank is warning customers to rotate all credentials and secrets stored on its platform after a security breach led to unauthorized use of customers’ AI API keys.

PHP2Shell Attacks Root Palo Alto Firewalls but Fail Against WordPress

SecurityWeek - 30 October 2026 16:09

Over 22.6 million exposed instances are potentially affected by the critical PHP flaws that have been targeted for over a week.

Cloudflare Reports 18.2 Million Network-Layer DDoS Attacks in Q3, Up 38%

The Hacker News - 31 October 2026 11:26

Threat actors are launching about 8,226 network-layer distributed denial-of-service (DDoS) attacks per hour, Cloudflare revealed Thursday. The web infrastructure and security company said it autonomously mitigated 18.2 million network-layer (L3) DDoS attacks and 14.4 trillion HTTP DDoS requests in the third quarter of 2026.

Binance Hit by Record-Breaking $6.3bn Hack in Largest Cryptocurrency Heist in History

Infosecurity Magazine - 30 October 2026 12:25

Leading cryptocurrency analysts have attributed the cyber-attack to a North Korean elite hacking unit.

Scottish Cyber Coordination Centre

NA

NA -

NA

NA -

NA

NA -

NA

NA -

NA

NA -

NA

NA -