Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 November 2026

Vulnerabilities

Critical Node-RED Flaw Exploited in Attacks

SecurityWeek - 03 November 2026 13:10

Multiple attacks from the same IP address attempted to deploy various payloads, including a Linux bot and webshells.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-119977 WordPress Core Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability

Barracuda warns of critical flaws allowing root access to devices

BleepingComputer - 03 November 2026 11:06

Cybersecurity company Barracuda Networks warned customers to patch two vulnerabilities that can let attackers run commands with root privileges.

Synology NAS Devices Targeted in Ransomware Attacks Exploiting Patched DSM Flaw

The Hacker News - 03 November 2026 14:13

Synology is urging customers to update the DiskStation Manager (DSM) software powering its Network Attached Storage (NAS) devices following ransomware attacks. The Taiwanese vendor said it observed threat actors exploiting a vulnerability patched in December 2024 to target devices running outdated versions of DSM.

Red Hat Patches 9.8-Rated Linux TCP RCE Flaw While Ubuntu Releases Fixes for Testing

The Hacker News - 03 November 2026 17:53

Fixed kernels for a use-after-free vulnerability in the Linux kernel's IPv4 TCP code are now available for Red Hat Enterprise Linux 8, 9, and 10, while Ubuntu's fixes for its three newest long-term-support releases remain in its opt-in testing channel with no date for a regular update.

Scottish
Cyber
Coordination
Centre

Scottish Cyber Coordination Centre

Threat actors and malware

Hackers hijack cPGuard autoupdate to deploy backdoor, steal data

BleepingComputer - 03 November 2026 18:18

Attackers have compromised the update infrastructure for the cPGuard web security suite to distribute a backdoor and a data-stealing script.

Russia-Aligned Gorbag Hackers Exploit WinRAR Flaw to Deploy Data-Stealing Malware

The Hacker News - 03 November 2026 17:30

A Russia-aligned threat actor known as Gorbag has been observed using simple information stealer malware in attacks targeting Ukrainian organizations.

UK Cyber Chief Says the UK Will Face AI Cyberattacks on Critical Infrastructure by 2028

SecurityWeek - 03 November 2026 10:49

The U.K. will likely face AI cyberattacks on its critical infrastructure by 2028 as criminals and states, including China and Russia, increasingly use AI in their cyber activity.

UK incidents

UK school estate hit by 3AM ransomware in suspected AI-assisted attack

BleepingComputer - 03 November 2026 10:00

A 3AM ransomware affiliate targeted a school estate in the UK and successfully encrypted around 37 of nearly 50 machines reached from an unmanaged host.

British businesses caught in Europe-wide supermarket fridge attacks

The Record from Recorded Future News - 03 November 2026 18:43

Three meat suppliers in Britain are among businesses that have been caught in a wave of cyberattacks across Europe targeting refrigeration systems, according to an industry trade body.