Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 November 2026

Vulnerabilities

VMware patches vCenter zero-day exploited in attacks since September

BleepingComputer - 19 November 2026 20:26

Broadcom has released security updates to fix a critical VMware vCenter Server authentication bypass vulnerability that Chinese-linked hackers have exploited in zero-day attacks since September 2026.

Hackers Exploit Cisco Expressway Vulnerability Soon After PoC Release

SecurityWeek - 19 November 2026 14:12

Attackers hacked clustered Cisco Expressway devices at a Russian organization and prepared tooling for lateral movement.

Critical PHP Flaws Allow Code Execution, But Don't Panic 'PHP2Shell'-Style

darkreading - 19 November 2026 20:57

November's monthly security release patches seven critical PHP flaws that should be addressed ASAP, though experts say exploitability varies and depends heavily on configuration.

Critical NGINX 'NGINX2Root' bugs let attackers hijack servers

BleepingComputer - 19 November 2026 10:57

Two critical NGINX vulnerabilities dubbed "nginx2root" allow unauthenticated attackers to execute code remotely on vulnerable web servers, with researchers demonstrating how the flaws can be chained with a Linux kernel bug to gain root access.

Drupal Patches Critical Installer Flaw That Could Give Unauthenticated Attackers Control of Sites

The Hacker News - 19 November 2026 21:03

Under specific conditions, a critical vulnerability in Drupal core can allow an attacker without login credentials to use the built-in installer to attempt to reinstall a site. That can lead to a site takeover or remote code execution, and the project rates the vulnerable configurations as uncommon.

Scottish Cyber Coordination Centre

ASUS warns of critical hard-coded key flaw in Control Center Express

BleepingComputer - 19 November 2026 17:15

ASUS released Control Center Express v1.7.29 to fix three critical vulnerabilities that could let remote attackers gain administrative control of the management console and the devices it manages.

Ruby Ships Fixes for 7 Flaws, Including Critical Ruby2Shell, Said to Hit Default Rails Apps Pre-Auth

The Hacker News - 19 November 2026 15:12

Ruby contains seven memory-safety flaws in its regular expression engine and its string case-conversion code. For five of them, its maintainers say, proof-of-concept exploits, or PoCs, have shown that crafted input can run code on the machine.

Critical Apache Roller, Axis Vulnerabilities Exploited in Attacks

SecurityWeek - 19 November 2026 13:13

Attackers are targeting Confluence Data Center through an Axis flaw and Apache is warning of attacks against Roller.

Splunk Patches Nearly 140 Flaws Across Three Core Products

SecurityWeek - 19 November 2026 11:41

The security updates resolve critical and high-severity issues leading to authentication bypass, remote code execution, and privilege escalation.

Threat actors and malware

ROMULUS ClickFix Attacks Deliver RAT That Can Spy on Users and Control PCs

The Hacker News - 20 November 2026 13:41

Threat actors have been observed using the ROMULUS ClickFix malware delivery platform to deliver a previously undocumented remote access trojan (RAT) that shares similarities with CNCMachineRMS.

Nvidia Responds to Gentlemen Ransomware Claim

SecurityWeek - 19 November 2026 15:17

Nvidia says it has found no indication that its systems were compromised after the Gentlemen ransomware group listed the company as a victim.

European Commission confirms cyberattack, says hackers used AI tool

The Record from Recorded Future News - 19 November 2026 16:15

The European Commission confirmed Thursday that it had been hit by a cyberattack last month involving a publicly available artificial intelligence tool, following media reports of the incident.

Scottish Cyber Coordination Centre

UK incidents

Transport for London breach exposes 265,000 Oyster card users' data

BleepingComputer - 19 November 2026 14:20

Transport for London (TfL) has announced that around 265,000 Oyster photocard customers may have had their account details exposed in a data breach.