Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 November 2026

Vulnerabilities

Threat Actors Exploit Openwave, Cisco BroadWorks Vulnerabilities

SecurityWeek - 11 November 2026 10:01

The flaws, CVE-2026-111793 and CVE-2026-20320, let attackers leak sensitive information, including configuration data.

Critical Xen Orchestra Flaws Exploited in Attacks

SecurityWeek - 11 November 2026 16:42

A critical authentication bypass allows attackers to execute arbitrary code as admin and take over XCP-ng nodes.

N-able releases security hotfixes for zero-day vulnerabilities

BleepingComputer - 11 November 2026 08:32

N-able released hotfixes to address zero-day bugs affecting its N-central remote monitoring and management (RMM) platform, which were publicly disclosed over the weekend and forced it to take vulnerable hosted environments offline.

Critical Apache HTTP/2 Flaw Could Let Unauthenticated Attackers Execute Code Remotely

The Hacker News - 12 November 2026 11:42

A critical flaw in Apache HTTP Server's HTTP/2 module, mod_http2, can let a remote attacker run code on the server. Tracked as CVE-2026-119618, it affects versions 2.4.55 through 2.4.70 and is fixed in version 2.4.71, released yesterday.

Critical Zoom Workplace Flaw Could Allow Unauthenticated Remote Privilege Escalation

The Hacker News - 11 November 2026 22:42

Zoom has released software updates to address two security flaws impacting Zoom Workplace for Windows, including a critical bug that could result in privilege escalation on affected systems.

Microsoft Fixes 1235 Flaws in Another Record Patch Tuesday

Infosecurity Magazine - 11 November 2026 10:15

Microsoft patched a record-breaking 1235 CVEs in November's Patch Tuesday

Scottish Cyber Coordination Centre

Citrix, Ivanti Patch Critical and High-Severity Vulnerabilities

SecurityWeek - 11 November 2026 14:37

Attackers could exploit the bugs to tamper with certificate entries, achieve remote code execution, and compromise hosts.

Fortinet Patches Nearly 100 Vulnerabilities

SecurityWeek - 11 November 2026 13:10

The massive drop comes after the company integrated frontier AI models into its product security testing.

Threat actors and malware

Active ScreenConnect attacks breach MSPs, impact dozens of organizations

BleepingComputer - 11 November 2026 18:56

ConnectWise is investigating an active malware campaign targeting managed service providers (MSPs) that uses compromised ScreenConnect environments to deploy rogue remote-access clients to customer devices.

AntiFox AI Pentesting Platform Linked to Attacks That Accessed AWS Production Secrets

The Hacker News - 11 November 2026 22:04

Cybersecurity researchers have disclosed details of a campaign in which an emerging agentic penetration testing platform called AntiFox has been used to steal Amazon Web Services (AWS) credentials and pivot laterally into compromised environments.

Hackers Target Qlik Sense Servers With Reverse Shells, Stage ActiveMQ and Veeam Exploits

The Hacker News - 11 November 2026 20:31

Threat actors have been observed targeting Qlik Sense servers to unsuccessfully deliver PowerShell reverse shell commands against multiple environments in October 2026. Cynet's CyOps and Research teams said they identified the suspicious activity in October 2026 against several E.U.-based customers within a narrow window of just over three minutes.

Suspected Chinese Malware Supplier Tied to Three Hacking Campaigns

Infosecurity Magazine - 11 November 2026 17:00

Check Point links three China-nexus clusters through a shared Sparrow malware framework.

Maersk confirms data breach as WhiteArmor ransomware demands $5 million

BleepingComputer - 11 November 2026 12:24

Maersk announced that a threat actor gained unauthorized access to a local legacy system inherited through an earlier acquisition and extracted data from it.

Scottish Cyber Coordination Centre

UK incidents

Iran-backed network directed London attacks over FaceTime, US prosecutors say

The Record from Recorded Future News - 11 November 2026 17:57

The U.S. accused three men of orchestrating attacks across Europe on behalf of Irans Islamic Revolutionary Guard Corps (IRGC), including a London arson incident that was recorded for propaganda.