Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 November 2026

Vulnerabilities

Microsoft November 2026 Patch Tuesday fixes 1,235 flaws, Outlook zero-day

BleepingComputer - 10 November 2026 15:07

Today is Microsoft's November 2026 Patch Tuesday, with security updates addressing a record-breaking 1,235 flaws, including one actively exploited Microsoft Outlook zero-day vulnerability.

Critical Xen Orchestra auth bypass flaw exploited to hijack VM servers

BleepingComputer - 10 November 2026 12:17

A critical authentication bypass vulnerability in Xen Orchestra is being actively exploited in attacks that could grant administrator privileges and allow takeover of XCP-ng virtualization hosts.

Binance warns of iOS flaw that could leak crypto wallet secrets

BleepingComputer - 10 November 2026 11:59

Binance is warning about a vulnerability in Apple's iOS 26.7.1, 27.0.1, and 27.2 that could allow third-party apps to read private files stored by other apps, including cryptocurrency seed phrases, secret keys, and login credentials.

SAP patches ICM2SHELL and PROXYGATE maximum severity flaws

BleepingComputer - 10 November 2026 08:07

SAP patched 35 vulnerabilities in its November 2026 security updates, including four maximum-severity issues affecting its NetWeaver, Web Dispatcher, and Gateway software.

Git Patches Flaw That Lets Malicious Repositories Execute Code During Recursive Clones

The Hacker News - 11 November 2026 01:53

A flaw in Git can let a malicious repository run an attacker's code on a computer that clones it recursively, together with its submodules. The Git project fixed it this week in Git 2.56.1, with matching fixes for the 2.50 through 2.55 series in 2.50.2, 2.51.3, 2.52.1, 2.53.1, 2.54.1 and 2.55.1.

Attackers Exploit AhsayCBS Flaws to Deploy Sandbox-Evading Python Backdoor

The Hacker News - 10 November 2026 22:30

Cybersecurity researchers have disclosed details of an attack that exploited two now-patched vulnerabilities in AhsayCBS to deliver a Python-based implant.

Scottish Cyber Coordination Centre

N-able Takes N-central Cloud Offline After Researcher Discloses 33 Zero-Days with PoC Exploits

The Hacker News - 10 November 2026 13:14

N-able said it has taken N-central Hosted Environments offline and is urging on-premises customers to shut down their servers until further notice following the public disclosure of over 30 vulnerabilities collectively tracked as Able2Shell.

Exploited Outlook Zero-Day Among 1,094 Flaws Patched by Microsoft

SecurityWeek - 10 November 2026 20:19

CVE-2026-124194 is the Outlook zero-day for which Microsoft says it's aware of active exploitation. The post Exploited Outlook Zero-Day Among 1,094 Flaws Patched by Microsoft appeared first on SecurityWeek.

CISA Adds Six Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-20320 Cisco BroadWorks Improper Restriction of XML External Entity Reference Vulnerability; CVE-2026-111560 Barracuda Networks Multiple Products OS Command Injection Vulnerability; CVE-2026-111793 Openwave Messaging Limited Webtop Media Transcoder Incorrect Resource Transfer Between Spheres Vulnerability; CVE-2026-116606 Barracuda Networks Email Security Gateway (ESG) Authentication Bypass Using an Alternate Path or Channel Vulnerability; CVE-2026-124194 Microsoft Office Outlook Missing User Interaction for Potentially Unsafe Action Vulnerability; CVE-2026-125350 Google Chromium Use-After-Free Vulnerability.

Threat actors and malware

Hackers exploit trusted AWS access to breach multiple cloud environments

BleepingComputer - 10 November 2026 15:31

A threat actor used compromised identity and access management (IAM) credentials for a Qubole big data platform's AWS account to access and exfiltrate data from multiple customers' AWS environments.

Hackers Exploit Critical Xen Orchestra Auth Bypass Flaw to Gain Admin Access

The Hacker News - 11 November 2026 00:42

French software company Vates VMS has warned of a critical security vulnerability in Xen Orchestra that it said is being actively exploited in the wild.The authentication bypass flaw, which does not yet have a CVE identifier, is tracked as VSA-2026-062.

Three China-Nexus Espionage Campaigns Linked Through Sparrow Malware Ecosystem

The Hacker News - 11 November 2026 00:13

Scottish Cyber Coordination Centre

Three distinct threat activity clusters with shared infrastructure and malware code similarities have been observed targeting telecommunications providers, government organizations, military entities, research institutions, and critical infrastructure across Latin America, Asia, and Europe over the past year.

Attackers Exploit AhsayCBS Flaws to Deploy Sandbox-Evading Python Backdoor

The Hacker News - 10 November 2026 22:30

Cybersecurity researchers have disclosed details of an attack that exploited two now-patched vulnerabilities in AhsayCBS to deliver a Python-based implant.

Anthropic's Claude Fable 5.2 Beats GPT-6 Cyber in Multi-Stage Cyberattack Benchmark

The Hacker News - 10 November 2026 14:46

Anthropic on Monday released Claude Fable 5.2 and Claude Mythos 5.2 models, which it said exhibit improvements in coding, reasoning, and vision.

Artex: The AI Pen-Test Tool Hackers Turned Into a Weapon

darkreading - 10 November 2026 22:01

Forks of the open source Artex framework, along with 45 similar pen-testing tools, remain capable of executing credential attacks and cloud breaches at machine speed across multiple industries.