It's Probably Nothing
by Sierra Echo Charlie

EDITION 27 / 13 NOVEMBER 2026

One cookie, a whole virtualisation fleet

Xen Orchestra's exploited bypass, Node.js memory leaks and AI intrusions with real consequences.

5 stories / Listen online - 3:59

THE TAKEAWAY

The Xen Orchestra disclosure deserves a catch-up: the distance between an authentication mistake and root on managed hosts is uncomfortably short.

01 / THE BRIEF

Xen Orchestra's bypass reaches beyond the appliance

On 10 November, Vates disclosed active exploitation of VSA-2026-062. An object-valued authentication cookie triggers an unfiltered token lookup, logging the attacker in as the first token's owner if it hasn't expired. Exploitation requires network access to Xen Orchestra; Vates says compromise can enable code execution across managed pools and root takeover of XCP-ng nodes.

Successful unauthenticated access leaves no application log identifying it, and missing campaign indicators don't establish a clean deployment. This isn't just an update-and-forget job.

WORTH ASKING

Fixed Xen Orchestra versions are 6.9.2 stable and 6.10.1 latest. For confirmed compromise, Vates recommends full reinstallation and rotation of virtualisation passwords and secrets.

SOURCES

VSA-2026-062: Empty-object login token - Primary source

Critical Xen Orchestra Flaws Exploited in Attacks - Reporting / context

Xen Orchestra Authentication Bypass Exploited to Hijack Virtualization Hosts - Reporting / context

02 / THE BRIEF

Node.js can leak across connections

Node.js's November security release fixes CVE-2026-123864, an HTTPS memory leak potentially exposing other users' requests and TLS private keys. The prerequisites are specific: a handler calls res.flushHeaders() before the request body ends, then res.end() with a non-empty chunk. Retrieving leaked memory also requires a route that echoes or stores a request body. Supported 22.x, 24.x and 26.x lines are affected; cleartext node:http isn't affected by this flaw.

The batch also fixes an HTTP/2 remotely triggered crash, a separate HTTP/2 response-memory leak and a cross-host client-certificate policy bypass. Application behaviour matters here, not merely having Node installed.

WORTH ASKING

Fixed releases are 22.23.5, 24.22.3 and 26.13.1.

SOURCES

Wednesday, November 11, 2026 Security Releases - Primary source

CVE-2026-123864 - Primary source

Node.js 26.13.1 (LTS) - Primary source

03 / THE BRIEF

AI intrusions, with production consequences

Unit 42's newly published investigation describes 25 operations against at least 19 organisations during August-September, with unauthorised access or data retrieval at 10. Attackers supplied targets and goals to a customised Cairn framework using Zhipu GLM and DeepSeek; humans could provide hints, and some tasks arrived with credentials or infrastructure details.

Unit 42 reports persistent administrator access at a semiconductor company and an overwritten live standards-ballot document elsewhere. Those outcomes are more interesting than another hacking demonstration. The reported techniques exploited established weaknesses, not novel ones.

QUALIFICATIONS

Victim confirmation wasn't obtained independently. Unit 42's China-nexus intelligence assessment carries moderate confidence.

SOURCES

Attackers Use Autonomous AI to Target Semiconductor, Defense and Civil Society Sectors - Primary source

Publisher API record for the CL-STA-1238 investigation - Primary source

Chinese-Speaking Attackers Use Autonomous AI Against 19 Organizations - Reporting / context

04 / THE BRIEF

One booking supplier, three states

ABC reports a Bookeasy incident affecting parks services in Queensland, Victoria and South Australia. South Australia says names, contact details and booking information may have been accessed. Parks Victoria reports suspicious WhatsApp messages and has suspended new campsite bookings; existing bookings remain valid, but modifications are unavailable.

The shared supplier has turned an investigation into a service interruption. Bookeasy told 7NEWS it detected unauthorised activity in early November and hadn't identified credit-card access.

SOURCES

Personal user data breached after Qld, Victoria and SA's National Park booking systems hacked - Reporting / context

Parks Victoria - News - Primary source

Customer details potentially exposed in national parks booking system breach across multiple states - Reporting / context

05 / THE BRIEF

Apache's HTTP/2 fix is worth catching up on

Disclosed on 11 November, CVE-2026-119618 is a critical mod_http2 synchronisation flaw that can cause heap corruption and remote code execution. Apache HTTP Server 2.4.55-2.4.70 is affected; 2.4.71 fixes it.

Wiz describes an unauthenticated path on HTTP/2 deployments, running at the web-server process's privileges-not automatically root. At publication, Wiz reported no available exploit or reports of exploitation.

SOURCES

CVE-2026-119618: Apache HTTP Server: mod_http2: heap corruption and RCE in assign_headers - Primary source

Apache HTTP Server 2.4 vulnerabilities - Primary source

Critical RCE Vulnerability in Apache HTTP Server: Everything You Need To Know - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.