It's Probably Nothing
by Sierra Echo Charlie

EDITION 32 / 20 NOVEMBER 2026

vCenter zero-day, PHP's fine print, Drupal installer

Google ties a vCenter auth bypass to an espionage crew; PHP and Drupal ship criticals

4 stories / Listen online - 5:21

THE TAKEAWAY

Plenty of things labelled critical today, but only one comes with a documented espionage intrusion attached. The rest are mostly a test of whether you know your own config.

01 / THE BRIEF

vCenter auth bypass was an espionage zero-day first, a patch second

Broadcom's VMSA-2026-0009 fixes CVE-2026-123890, an authentication bypass in the VMware Directory Service rated 9.8, with no workaround and credit to Mandiant. On the same day, Google Threat Intelligence Group said ARMORY CASTLE, a suspected PRC-nexus espionage actor formerly tracked as UNC5221, used it as a zero-day in early September with a Go tool it calls BONESAW.

Google's write-up is the bit worth reading. An unauthenticated SRP session-key disclosure over DCE/RPC on port 2012 yields an administrator@vsphere.local session. From there BONESAW pulls the STS SAML signing key and creates an SSO admin, and a companion tool, SAWSNAKE, does Golden SAML to skip MFA and impersonate anyone. In the intrusion Google investigated, the actor came in through a BeyondTrust Remote Support appliance compromised via the earlier zero-day CVE-2026-102764. It hopped to an internal Linux box without EDR, then took vCenter, ESXi root and NTDS.dit from VM disks. That's the whole estate, more or less.

Fixes are vCenter 9.1.1.0200, 9.0.2.0200, 8.0 U3m and VCF 5.2.5. vCenter 7.0 customers need to go through extended support. The Hacker News reports that Broadcom's FAQ calls this an emergency change and says 6.5 and 6.7 should be presumed affected.

It needs network access to vCenter, which sounds reassuring until you remember that the attacker's whole job is getting inside the network first. My read: with a stolen signing key in the mix, patching alone probably isn't the end of the story if you think you've been visited.

WORTH ASKING

Beyond the patch, Google suggests allowlisting inbound access to ports 2012, 443, 22 and 5480, plus egress filtering and remote logging.

QUALIFICATIONS

The exploitation evidence comes from Google's investigation of a single intrusion. Broadcom itself hasn't reported attacks, per The Hacker News. Google notes BONESAW's 13 July build timestamp predates July's CVE-2026-59309 disclosure, but cautions that Go build metadata can be altered.

SOURCES

VMSA-2026-0009: VMware vCenter, Tools, and SDDC Manager updates address multiple vulnerabilities - Primary source

ARMORY CASTLE Exploits vSphere - Primary source

Critical VMware vCenter Flaw (CVSS 9.8) Lets Network Attackers Bypass Authentication - Reporting / context

ARMORY CASTLE Exploits VMware vCenter Flaw in Espionage Intrusion - Reporting / context

02 / THE BRIEF

PHP's critical RCEs come with plenty of conditions

PHP 8.5.13, 8.4.28, 8.3.37 and 8.2.36 landed on 19 November, with three critical advisories. These are new bugs, not a bypass of October's PHP2Shell fixes, and PHP itself says the critical ones need non-default or uncommon setups.

The practical one is PHP-FPM request smuggling. If the front end reuses backend connections (nginx fastcgi_keep_conn on, Apache enablereuse=on, or HAProxy keeping connections open) and the app opens php://input without reading it fully, the leftover bytes become a forged request controlling SCRIPT_FILENAME and PHP_ADMIN_VALUE. That's unauthenticated code execution in one request, with no memory corruption needed. Standard close-after-each-request configs aren't hit by the demonstrated attack, and the code has been there since 5.6.0.

The other two are much fussier. A timezone-cache use-after-free has only demonstrated code execution locally, and PHP calls a remote ASLR bypass plausible but unproven. A session-file race needs attacker-influenced session data, well-timed interruption and a gadget chain.

WORTH ASKING

If you've switched on FastCGI keep-alive for performance, that's the box to check first. PHP's interim fix is to turn off reuse and keep FPM and LSAPI listeners away from untrusted networks.

QUALIFICATIONS

The advisories describe no in-the-wild exploitation.

SOURCES

PHP: News Archive - 2026 - Primary source

PHP-FPM request smuggling through an unread HTTP request body - Primary source

Timezone cache use-after-free can lead to remote code execution - Primary source

Partially overwritten session files can lead to remote code execution - Primary source

03 / THE BRIEF

Drupal's installer can be pointed back at a live site

SA-CORE-2026-017, dated 18 November, covers CVE-2026-132165. Under specific conditions, an anonymous attacker can use install.php to attempt a reinstall, leading to site takeover or RCE. Drupal rates it Critical (18/25) with proof-level exploit maturity but complex, uncommon conditions. Fixes are 10.6.22, 11.3.22 and 11.4.13. Anthropic's OSS Scanner found it, which is becoming a familiar credit line.

BleepingComputer quotes Drupal's advance warning that exploits might appear within hours or days.

WORTH ASKING

If you can't upgrade immediately, lock down the installer. A settings.php the web server can't write to or re-permission also blunts some paths.

QUALIFICATIONS

No active exploitation has been reported.

SOURCES

Drupal core - Critical - Remote code execution - SA-CORE-2026-017 - Primary source

Drupal patches critical RCE flaw, warns exploits may surface quickly - Reporting / context

Drupal Patches Critical Installer Flaw That Could Allow Site Takeover - Reporting / context

04 / THE BRIEF

KEV catches up with LiteLLM and REDCap

CISA's 18 November KEV batch confirms exploitation of LiteLLM's custom-code guardrail sandbox escape, CVE-2026-40217, which was patched back in May. It needs a proxy-admin credential by default, but the proxy runs as root in the default Docker image, and gateways like this tend to hold everyone's provider keys. The advisory contradicts itself on whether the fix is in 1.83.10 or 1.83.11, so go to 1.83.11 or later, or block POST /guardrails/test_custom_code.

REDCap CVE-2026-90817 is unauthenticated code injection from a public survey context, provided the attacker knows a valid survey hash. CISA wants forensic triage on that one. Synology CVE-2024-10441 and the already-reported Apache Axis bug also made the list.

QUALIFICATIONS

Neither the exploitation details nor the victims are public, and REDCap's own guidance wasn't reviewed.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities (JSON) - Primary source

CISA Adds Four Known Exploited Vulnerabilities to Catalog - Primary source

LiteLLM has a sandbox escape in custom-code guardrail · CVE-2026-40217 - Primary source

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.