It's Probably Nothing
by Sierra Echo Charlie

EDITION 21 / 5 NOVEMBER 2026

Your WordPress site is most hackable while updating it

Plus: cPGuard's own update channel shipped a backdoor, and APT29's mobile watering holes get an autopsy.

5 stories / Listen online - 7:42

THE TAKEAWAY

Busy one today. Two of the bigger stories involve update infrastructure being turned against its owners - one in WordPress core itself, one at a security vendor - plus a pair of genuinely good research drops from Sekoia and ESET, and a local warning worth forwarding to the less technical people in your life.

01 / THE BRIEF

WordPress core's upgrade window is now a KEV-listed RCE

CISA has added CVE-2026-119977 to the Known Exploited Vulnerabilities catalogue, based on evidence of active exploitation. It's a TOCTOU race condition in WordPress core's own upgrade process: during a full-package upgrade, predictable, web-accessible staging paths let an unauthenticated attacker execute code on the server. The important caveat is the timing - this is only exploitable while a site is mid-upgrade, not a standing pre-auth RCE. But that's a window a huge chunk of the self-hosted web passed through recently, because the fix only shipped on 28 October in WordPress 7.1.4 (credited to reporter Umut Bayram, alongside a pile of mostly stored-XSS fixes). CISA's given US federal agencies until 6 November and flagged forensic triage as required, which is unusually brisk. Known ransomware campaign use is listed as Unknown.

Wordfence's entry describes the affected range as 4.7.0 through 7.1.3 - effectively the entire fleet - though their detail page returned a 403, so that range comes from the entry's title rather than the full text. WordPress says backports are being shipped to all eligible branches down to 4.7 as they become ready, but only the latest version is actively supported.

WORTH ASKING

If you run WordPress and did a full-package upgrade before 7.1.4 landed, the forensic triage language in the KEV entry is aimed at you. Patch, and have a look at what happened during the upgrade window.

QUALIFICATIONS

No attack detail, actor or victim count is public beyond CISA's statement that exploitation is happening.

SOURCES

CISA Adds One Known Exploited Vulnerability to Catalog - Primary source

CISA Known Exploited Vulnerabilities Catalog (CSV) - Primary source

WordPress 7.1.4 - Primary source

02 / THE BRIEF

cPGuard's autoupdate pushed a backdoor to ~2,900 servers

OpsShield says an attacker used compromised credentials to get into its update distribution CDN at 02:06 UTC on 2 November, and used the cPGuard update channel itself to push a malicious script. Versions 5.88.12 through 5.88.19 are affected. The script installed a backdoor and collected Linux password hashes, root MariaDB/MySQL configuration, root shell history and root SSH files - exfiltrated, with a certain poetry, through OpsShield's own licensing server via a compromised account. The vendor told BleepingComputer 2,946 servers were affected and had that data copied, and that its billing system database went too. OpsShield says it detected the compromise and stopped distribution within 12 hours, and that some servers escaped because update checks run at intervals. How the credentials were obtained in the first place remains unclear.

cPGuard is a security suite commonly bolted onto cPanel, DirectAdmin and Plesk boxes by hosting firms - the kind of software that's supposed to be the solution to this sort of problem. Root credential theft across thousands of shared-hosting servers has obvious second-order potential.

WORTH ASKING

Version 5.88.25 removes the backdoor and staged files, but the collected credentials are already gone - passwords, database creds, cloud secrets and SSH keys all need rotating, not just patching over.

SOURCES

Hackers hijack cPGuard autoupdate to deploy backdoor, steal data - Primary source

cPGuard Update Channel Hijacked to Deploy Backdoor and Steal Server Credentials - Reporting / context

03 / THE BRIEF

APT29's mobile watering holes: cookies, keychains and a hijacked analytics firm

Sekoia has published a thorough autopsy of a watering-hole campaign it uncovered in mid-October, and the most interesting part isn't the exploits - it's the plumbing. Three delivery vectors: compromised legitimate sites, lookalike reverse-proxy domains for america250.org and Raffles London at The OWO (the hotel near Whitehall where, per open-source reporting, Zelensky stayed on 14 October), and a one-week trojanisation of Ukrainian analytics service Plerdy's tracker between 27 August and 3 September, which exposed hundreds to thousands of predominantly Ukrainian sites including defence-sector and military-recruitment pages. Visitors on outdated iOS or Android got zero-click chains built entirely from known, patched vulnerabilities - no zero-days - including a full-device iOS 18.5 chain reusing the DarkSword commercial surveillance kit. Payloads stole browser cookies and, in some cases, message stores, keychain items and Wi-Fi passwords, with no persistence installed. Stolen session cookies mean webmail access without a password.

Sekoia assesses APT29 (SVR) with moderate-to-high confidence, citing technical overlaps and victimology; Google TAG confirmed the framework resembles APT29's 2024 Mongolian watering-hole work and that the exploits match commercial surveillance vendor tooling. A state actor shopping from the CSV catalogue is becoming a pattern. Fully updated devices were never at risk - this one punished the unpatched.

QUALIFICATIONS

Attribution is Sekoia's assessment, moderate-to-high confidence, with Google TAG corroboration.

SOURCES

Poisoned Source: APT29 watering holes target mobile devices with n-day exploits - Primary source

Suspected Russian SVR Campaign Targets Mobile Devices to Steal Login Cookies - Reporting / context

04 / THE BRIEF

Sogou's insecure config fetch became a DarkVigil delivery service

ESET has detailed a DNS hijacking operation by SlippyNunchucks, the China-aligned group behind the DarkVigil toolset. Since 1 July, whoever controlled DNS resolution for config.pinyin.sogou.com could answer the Sogou Input Method's unencrypted HTTP brand-promotion requests with a malicious configuration, telling the legitimate SGTool.exe to fetch a signed Adobe binary and a malicious libcef.dll - then plant them where Sogou's own component workflows would side-load the implant. Persistence without ever installing a persistence mechanism, at the cost of breaking Sogou's software in the process, which ESET dryly notes is destructive. Victims turned up in Hong Kong, Thailand, Japan, Vietnam, Sri Lanka and Oman, including a multinational gambling organisation, a Dubai internet café and, for some reason, a Danish university student. Tencent's version 16.10 moves the requests to HTTPS with certificate pinning, and ESET's CNA issued CVE-2026-120422 on 2 November.

The unsettling part is that nobody knows where the DNS manipulation happens - compromised routers, router implants or ISP-level interception are all on the table. ESET also notes the fix leaves residual gaps: SGTool.exe still doesn't validate downloaded file types or restrict destinations.

WORTH ASKING

Anyone with Sogou IME in the environment should be on 16.10, and the IoCs are worth a look.

QUALIFICATIONS

ESET's post is internally inconsistent on the fix date (29 October in the body, 30 October in the timeline box). The surveillance-alignment judgement is ESET's high-confidence assessment; the group is distinct from Mustang Panda in their telemetry.

SOURCES

SlippyNunchucks hijacks Sogou Input Method's brand promotion mechanism to distribute malware - Primary source

SlippyNunchucks Exploits Sogou DNS Hijacking to Deploy DarkVigil Surveillance Malware - Reporting / context

05 / THE BRIEF

NCSC: the fake job app wants your Accessibility permissions

A short local one to finish. New Zealand's NCSC is warning that malicious actors are distributing Android malware disguised as a job-seeking app, pushed through social media and chat messages, sometimes with a follow-up phone call for that personal touch. Sideload it and you get a fake Google Play update page for legitimacy, then a request for Accessibility permissions - grant those and the scammer effectively owns the device. The NCSC notes the same malware also poses as banking apps, and its recovery advice runs to a factory reset, because the thing can install further malware and a plain uninstall may not cut it. No family name or actor attribution, so don't read more into it than that.

SOURCES

Fake job app installs malware on Android phones - 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.