It's Probably Nothing
by Sierra Echo Charlie

EDITION 35 / 25 NOVEMBER 2026

Cyberattack knocks South Island papers off press

WordPress.org stops six bad updates, and CISA calls for forensic triage.

5 stories / Listen online - 3:13

THE TAKEAWAY

A cyberattack at Allied Media meant some South Island papers didn't come out at all. There's a more encouraging story from WordPress.org, where six backdoored plugin updates made it into the repositories but didn't make it out of the directory.

01 / THE BRIEF

Allied Media cyberattack stops two West Coast editions

Allied Media told RNZ a cyberattack disrupted several production systems. The Greymouth Star's deputy editor said Tuesday's Greymouth Star and Wednesday's Hokitika Guardian couldn't go ahead. Allied Media pushed Wednesday deliveries of the Blenheim Sun, Southern Rural Life and The Ensign to Thursday.

Allied Media was still working to restore access to produce Wednesday's Otago Daily Times when RNZ reported. The company said it had no evidence customer information had been accessed, but that was an interim finding.

SOURCES

Newspapers delayed as Allied Media hit by cyber attack - Reporting / context

02 / THE BRIEF

MONAI Label's fix is out, but exposed servers need a look

CISA added CVE-2026-133968 to its Known Exploited Vulnerabilities catalogue and called for forensic triage, with a 26 November deadline for covered US federal agencies. MONAI Label through 0.8.5 is affected, and authentication is off by default. AWS had already reported exploitation in a September campaign targeting East Asian universities; the CISA listing is the new bit.

WORTH ASKING

Upgrade to 0.8.6. If the older server was reachable from an untrusted network, the maintainers recommend checking for unexpected file changes before bringing it back into service.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

CISA Adds Two Known Exploited Vulnerabilities to Catalog - Primary source

Path traversal in datastore upload endpoints allows arbitrary file write - Primary source

MONAI Label 0.8.6 - Primary source

Chinese-nexus actor's Cairn AI agents found a zero-day on their own - Primary source

03 / THE BRIEF

WordPress.org holds back six backdoored plugin updates

Wordfence says WordPress.org's release hold and automated reviewer stopped malicious updates to six WP connect plugins before the directory distributed them. All six plugins were closed. The plugins had more than 3,600 active installations between them, according to Wordfence. That's the size of the installed base, not a victim count.

WORTH ASKING

There's no patched release. If you ran a version listed under CVE-2026-135202, Wordfence recommends removing it, scanning the site and rotating administrator passwords and secret keys. Removing the plugin alone may not clear a compromise.

SOURCES

CVE-2026-135202 - Wordfence CNA record - Primary source

Supply Chain Compromise Backdoors Six WP connect Plugins, Blocked by WordPress.org's Release Hold - Primary source

04 / THE BRIEF

Mail Assure flaw joins the known-exploited list

The same CISA update added CVE-2026-134624, affecting Mail Assure and SpamExperts, with the same forensic triage requirement and 26 November deadline for covered US federal agencies. N-able had already restored dashboard and API access, and says mail flow and filtering continued throughout. The listing establishes exploitation of the flaw, not that it was how the attacker got into N-able's hosted server.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

Mail Assure Incident Update - Primary source

CISA warns of exploited N-able bug as company restores email platform - Reporting / context

N-able Server Breach Disrupts Mail Assure and SpamExperts Management Across Three Regions - Reporting / context

05 / THE BRIEF

Unit 42 puts a stopwatch on AI-led intrusions

In a subset of attacks Unit 42 analysed, the median gap between commands fell from 23.9 seconds under manual control to 1.4 seconds after an agent took over. Humans still provided strategic oversight, and the observed behaviour alone couldn't identify a specific model or framework.

That's not a speed estimate for every intrusion. It's a concrete example of how much less time defenders can have to contain one after the handover.

SOURCES

Recent Trends and Tactics of Agentic AI Attacks - Primary source

Unit 42 publisher API - publication metadata - Primary source

AI Agents Accelerate Web Application Intrusions and Post-Exploitation - 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.