It's Probably Nothing
by Sierra Echo Charlie

EDITION 34 / 24 NOVEMBER 2026

GL.iNet's cloud backdoors routers, Drupal exploited

Plus a leak from the Commission's month-long intrusion, N-able's CVE and an ASX trading halt.

5 stories / Listen online - 4:12

THE TAKEAWAY

The pick of today is a vendor's own remote-management cloud being used to put root-level malware on its customers' routers and KVMs. Elsewhere, a Drupal bug we covered last week is now reported exploited, and the European Commission's intrusion has started leaking user data.

01 / THE BRIEF

GL.iNet's cloud pushed malware to its own routers and KVMs

GL.iNet says someone exploited a flaw in its cloud remote-management service, identified on 20 November, to get into some of its routers and KVM devices and install malware. The cloud side is fixed, so there are no new infections by that route. Devices that were already infected stay infected until they get the new security firmware.

The KVM part is the nasty bit. GL.iNet says it's still working out whether computers plugged into affected KVMs were hit, and wants owners of infected units to check them.

RemoteToHome Consulting, a GL.iNet services partner, says 166 of the 199 routers it reached showed the 20 November attack, an older backdoor, or both. It can't say how those older backdoors got there. That's one partner's managed fleet, not a population estimate. It thinks a command-injection flaw in the GoodCloud client was the way in, but GL.iNet hasn't confirmed that. BleepingComputer's malware analysis found persistence, optional SSH key installation and a swapped-out netstat that hides the malware's connections. Nobody knows who did it or how many devices are affected.

WORTH ASKING

If you have GL.iNet gear, install the cleanup firmware even if the quick check comes back clean. GL.iNet admits that check can miss newer indicators. Examples include 4.11.1 or later for GL-MT3000 and GL-MT6000, 4.8.4 for GL-AXT1800, 4.7.14 for GL-MT2500 and 1.10.3 for most Comet KVMs. An unlisted model isn't necessarily safe. Cleaning the device doesn't revoke anything that was stored on it, so rotate any keys, passwords and VPN profiles at the other end.

SOURCES

GL.iNet Security Notice 2026-11-20 - Primary source

Hackers exploit GL.iNet cloud flaw to infect routers, KVM devices - Reporting / context

GL.iNet Routers, KVMs Compromised via Remote Management Service Flaw - Reporting / context

GL.iNet cloud compromise hits routers and KVMs, older backdoors also found - Reporting / context

Attackers Exploit GL.iNet Cloud Flaw to Install Malware on Routers and KVMs - Reporting / context

02 / THE BRIEF

Drupal's install.php bug has moved from proof-level to exploited

When we covered SA-CORE-2026-017 (CVE-2026-132165) on 20 November, there were no reported attacks. Drupal now says its Security Team has received a report of exploitation on live sites as early as 19 November at 19:00 UTC. It has raised the rating to Highly critical, 20/25. The vector still lists complex access and uncommon targets, so most sites aren't in scope. There's still no victim count.

The fixes are unchanged: 10.6.22, 11.3.22 and 11.4.13. A settings.php the web server can't write to blocks some exploit paths but not all of them.

WORTH ASKING

Anyone who left install.php reachable and hasn't patched should look for signs of compromise, not just patch.

SOURCES

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

Drupal Security Team Reports Installer Flaw Exploited on Live Sites - Reporting / context

03 / THE BRIEF

European Commission intrusion leaks EU Academy user data

The Commission has confirmed that names and email addresses of EU Academy users leaked, and has warned them to expect phishing. Euronews reports the intrusion was detected on 22 October and still isn't fully contained a month later. Citing two unnamed sources, it says the Commission suspects a China-backed network, based on the attack's sophistication and its use of the AI-driven ARTEX tool. Spokesperson Thomas Regnier says the Commission won't attribute anything until the investigation ends.

SOURCES

Exclusive: China-backed hackers suspected behind ongoing EU Commission cyberattack - Reporting / context

European Commission warns EU Academy users of data leak after AI-driven cyberattack - Reporting / context

European Commission Cyberattack Disrupts HR, Reimbursement and Translation Services - Reporting / context

04 / THE BRIEF

N-able restores Mail Assure and names the bug

N-able restored the Mail Assure and SpamExperts dashboards and APIs on 21 November and published CVE-2026-134624. SecurityWeek describes it as a CVSS 9.3 SSRF in the LDAP sync connection check, reachable by a sufficiently privileged API user and fixed in version 20261121.1943. N-able says it has found no exploitation beyond one hosted server. It hasn't explicitly said this CVE was the way in. A root-cause analysis is due within two weeks.

SOURCES

Mail Assure Incident Update - Primary source

N-able Patches Critical Flaw Disclosed After Mail Assure Cyberattack - Reporting / context

CVE-2026-134624 - MailAssure LDAP sync connection check SSRF - Primary source

05 / THE BRIEF

Peninsula Energy halts ASX trading over a uranium-site incident

Peninsula Energy requested a trading halt on 23 November over a cyber incident late on 20 November (AWST) at its Lance Project in Wyoming. It says operations will be temporarily affected. It describes the breach as limited to its 'operating system', with its US and Australian administrative systems untouched. What that phrase actually means is anyone's guess until the promised announcement.

SOURCES

Trading Halt - Peninsula Energy Limited (ASX:PEN) - Primary source

AngloGold, Peninsula disclose mining cyber incidents - 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.