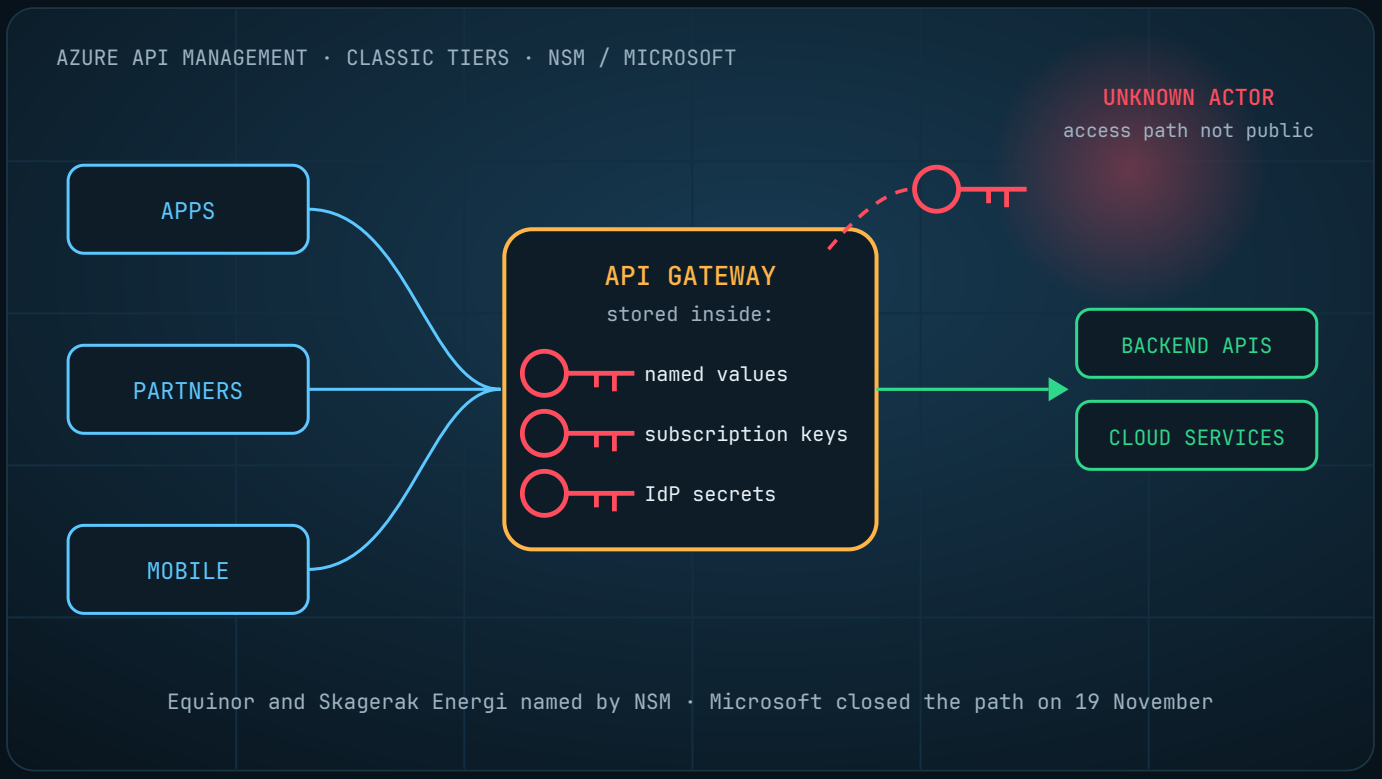
MAG212
CYBER

DAILY

Tuesday, 24 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 7:00 AM PT



AZURE API MANAGEMENT · NORWAY · ENERGY SECTOR

The keys behind the gateway

An unknown actor went after the tokens and secrets stored in Azure API Management. Microsoft closed the hole on 19 November, but the stolen keys still work until you rotate them. Also: a cloud bug let attackers run commands on GL.iNet routers and KVMs.

03 Secrets lifted from Azure API gateways
04 Check, hunt and rotate: APIM playbook
05 GL.iNet's cloud hands out root
06 Cleaning a router or KVM you can't trust
07 phpAfterShell: one torn session file
08 AI agents find a zero-day in 11 minutes
09 Patch board and KEV deadlines

ROTATE
every APIM secret and named value

v3.19.14
GoodCloud fix; firmware per model

8.2.36+
PHP fix for phpAfterShell

26 NOV
KEV due: MONAI, Mail Assure

What matters today

Developments published or updated 22–24 November. Theme: the keys inside your vendors' clouds.

Cloud gateways leak their keys

Norway's NSM says an unknown actor targeted tokens and secrets in Azure API Management, naming Equinor and Skagerak Energi. Microsoft says Classic-tier customers were exposed. [1][2]

A vendor cloud reaches your devices

A message-authorisation error in GL.iNet's GoodCloud let an attacker send management commands to other users' routers and KVMs and install malware. [6][8]

Machines find the bugs now

Amazon says a China-nexus actor's AI agents found and exploited a MONAI Label zero-day in about 11 minutes. CISA added it to KEV on 23 November. [13][16]

Old code, new tricks

phpAfterShell revives October's PHP2Shell path through a session file that PHP rewrites without clearing. Fixed 19 November; no attacks reported. [9][10]

THE THREE PRIORITY ACTIONS

1. **Rotate every secret held in Azure API Management Classic instances.**
   Named values, IdP secrets, subscription keys, backend credentials; then check each gateway's RuntimeVersion. [1]
2. **Update GL.iNet routers and KVMs; rebuild any that look compromised.**
   If you suspect access, flash without keeping settings and replace stored VPN and SSH keys. [6]
3. **Close KEV: four items due today, two more on Thursday.**
   Outlook, Chromium, BroadWorks and Openwave are due 24 November; MONAI Label (0.8.6 is out) and Mail Assure on 26 November. [15][16]

STATUS AT A GLANCE

ISSUE	STATUS	FIX / NEXT STEP
Azure APIM Classic (no CVE)	EXPLOITED · CLOSED 19 NOV	rotate secrets; check build
GL.iNet GoodCloud (CVE pending)	EXPLOITED · CLOUD FIXED	security firmware
MONAI Label CVE-2026-133968	EXPLOITED · KEV	0.8.6 · due 26 Nov
PHP CVE-2026-126714	POC ONLY · NOT IN KEV	8.2.36+ per branch

CONTENTS

03 Azure API Management secrets
04 APIM: check, hunt, rotate
05 GL.iNet GoodCloud compromise
06 GL.iNet: investigate and rebuild
07 phpAfterShell (CVE-2026-126714)
08 AI agents and the MONAI zero-day
09 Patch board
10 Briefs
11 Defender's Action Desk
12 Awareness: cloud dashboards
13 Sources

AZURE API MANAGEMENT · CLASSIC TIERS · NO CVE

Secrets lifted from Azure API gateways

Norway's security authority says an unknown actor targeted the tokens and secrets that API Management stores. Microsoft has closed the access path, but anything taken still works until it is rotated.

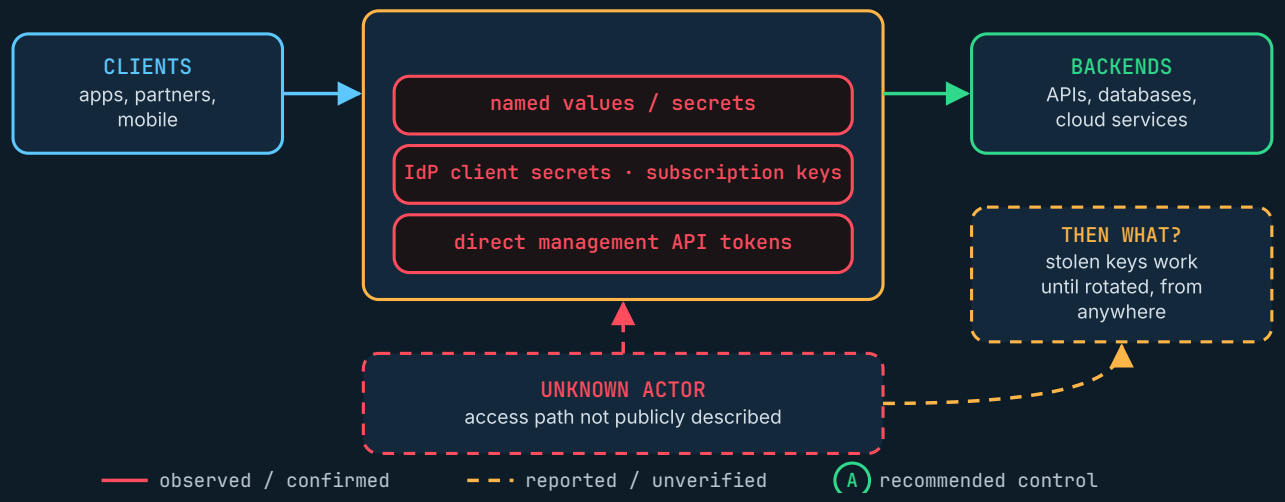


Figure 1 · What sits inside an APIM instance and why theft matters. The access path is not public, so it is shown dashed. MAG212 CYBER diagram from NSM and SecurityWeek [1, 2].

WHAT HAPPENED

On 20 November Norway's National Security Authority (NSM) said an unknown actor had "actively" gone after access tokens, secrets and named values in Azure API Management (APIM). Several Norwegian organisations in more than one sector were affected, plus some abroad; NSM names Equinor and Skagerak Energi. The energy sector spotted it first. NSM has seen no effect on deliveries. [1]

Microsoft found the issue on 18 November and closed it on 19 November. Its customer notice, reported by SecurityWeek, says customers "were exposed" and an unauthorised party could have used the issue. Only Classic-tier instances not following Microsoft's security guidance are affected; v2 and Consumption tiers are not. [2][4]

WHAT IS NOT KNOWN

- How the actor reached the secrets. No CVE, advisory or indicators are public.
- How many tenants were touched, and whether secrets were used.
- Who the actor is. NSM names no group or country.

WHO IS AFFECTED

- APIM **Classic** tiers (Developer, Basic, Standard, Premium) not hardened per Microsoft guidance [2].
- Anything whose credentials APIM stored: backend APIs, identity providers, partner subscriptions.
- Equinor reported its incident on 17 November and found no data stolen; Skagerak saw no operational impact [2].

WHY IT MATTERS

An API gateway is a vault of other systems' keys. The cloud fix stops new theft, but cannot recall keys that already left. Every secret APIM held has to be treated as public until replaced. (MAG212 analysis)

STATUS Exploited, per NSM and Microsoft. Service-side fix in place since 19 Nov. Customer rotation still required.

The APIM playbook: check, hunt, rotate, harden

Work in this order. Rotation is the step that actually removes the risk; the rest tells you how far it went.

Any OS · browser or curl | none

READ-ONLY | NOT TESTED BY MAG212

1 · is the gateway patched?

```
curl -s https:///internal-status-0123456789abcdef
```

Read RuntimeVersion: 0.52.x is patched from 31936, 0.53.x from 31938. Other patterns mean v2/Consumption (not affected). Lower: contact Microsoft. From NSM [1]; not tested by MAG212.

2 · ROTATE, IN THIS ORDER

1. Assume every secret and named value in APIM is compromised [1].
2. Backend credentials and app-registration client secrets.
3. Subscription keys; tell partners before you cut over.
4. Key Vault secrets APIM references, and tenant access keys.
5. Map what sat behind each instance so you know your exposure.

Microsoft's guide: Rotating credentials in Azure API Management [5].

3 · HUNT: LOG SOURCES AND WHAT TO LOOK FOR

LOG SOURCE	LOOK FOR
AzureActivity	listSecrets, named-value, policy, IdP and user writes you did not make
APIM gateway logs / AzureDiagnostics	new subscription IDs; requests with tracing enabled
APIMDevPortalAuditDiagnosticLog	sign-ups or sign-ins on the old developer portal
AADServicePrincipalSignInLogs	APIM-linked app registrations signing in from new IPs
AZKVAuditLogs	SecretGet / SecretList by unexpected callers
MicrosoftGraphActivityLogs	Graph calls by APIM-linked apps (Entra ID P1/P2)

From independent researcher Anders Kristiansen [3], who notes this may not be the vector NSM described. Treat as hunting leads, not indicators.

A LEAD WORTH CHECKING

Kristiansen points to APIM's retired direct management API (`*.management.azure-api.net`). It signs in with SharedAccessSignature tokens, skips Entra ID and RBAC, and its calls do not show in the Activity log. He does not claim it was the attack path. [3]

4 · HARDEN

- Set “Enable Management REST API” to No.
- Unpublish or lock down the legacy developer portal and its sign-up providers.
- Limit who can edit policies or turn on request tracing.
- Move instances to v2 tiers where you can.

Hardening steps from Kristiansen [3]; tier move is MAG212's suggestion.

HOW TO KNOW YOU ARE DONE

Every gateway shows a patched RuntimeVersion; old secrets fail when tested; no unexplained management writes or new subscriptions in your log retention window. In Norway, report signs of compromise to NCSC (cert@ncsc.no) [1].

GL.iNET · GOODCLOUD · CVEs PENDING

GL.iNet's cloud handed attackers a remote control

A permission error in the vendor's remote-management service let an attacker send commands to other customers' routers and KVMs. GL.iNet says malware was installed on some.

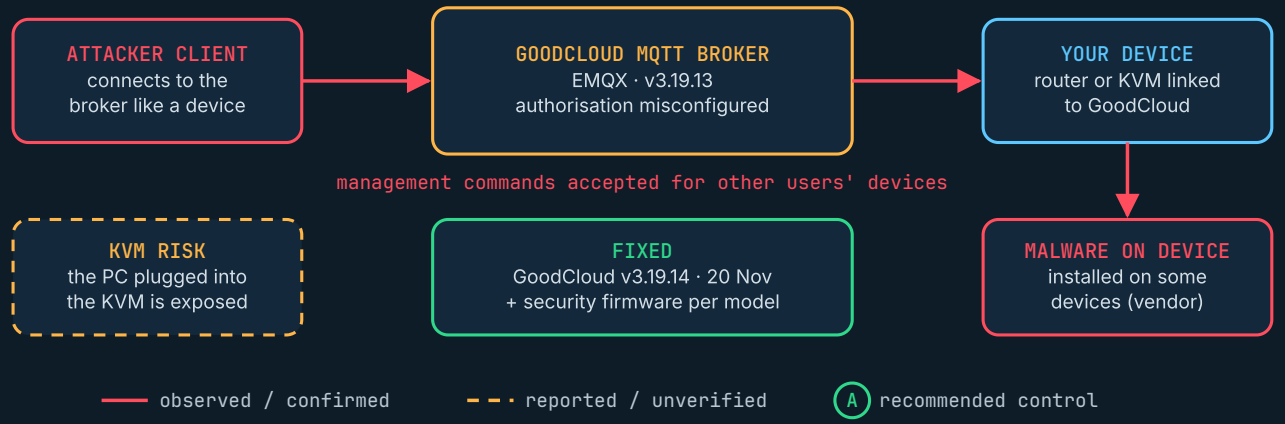


Figure 2 · The GoodCloud attack path as GL.iNet describes it [6]. The KVM risk to attached computers is the vendor's own warning. MAG212 CYBER diagram.

WHAT HAPPENED

On 20 November GL.iNet found that "an unauthorized party exploited a vulnerability" in GoodCloud, its remote-management service. The flaw was a message-authorisation error in the MQTT broker (EMQX) that relays commands to devices. GL.iNet fixed the service (v3.19.14), blocked the path the same day and shipped security firmware. It has not said how many devices were hit or who did it. [6]

TWO MORE FLAWS IN THE FIRMWARE

The notice also lists a root command injection in AstroWarp/SD-WAN management on routers (reportedly reachable even with AstroWarp off) and a TLS-verification bypass in the KVMs' RTTY remote terminal. CVE numbers are pending. [6]

REPORTED, NOT CONFIRMED BY THE VENDOR

A community analysis describes a root reverse shell to 170.39.226.219 from about 21:40 UTC on 20 November and a KVM implant called "gl-helper". SecurityWeek reports that most of nearly 200 routers the group checked looked affected, some by an older backdoor. [7][8]

MINIMUM SECURITY FIRMWARE

MODEL	MIN. FIRMWARE
GL-MG1300, GL-MT3000, GL-MT6000	4.11.1
GL-E5800	4.10.3
GL-BE3600, GL-BE9300	4.10.2
GL-BE14000	4.9.3
GL-BE6500, GL-MT3600BE, GL-MT5000	4.9.1
GL-BE10000	4.8.7
GL-AX1800, AXT1800, SFT1200, X3000, XE3000	4.8.4
GL-MT2500/A, GL-X2000	4.7.14
KVM RM1, RM1V2, RM10, RM10RC, RM1PE, RM4PE	1.10.3
KVM RMQ1	1.8.7

From GL.iNet's notice [6]. Install the latest stable release for your exact model; the list is not a list of compromised devices.

Cleaning a router or KVM you can't trust

Updating firmware closes the holes. It does not remove what an attacker already installed. Here is the order of work for owners and MSPs.

IF YOU USED GOODCLOUD

1. Install the security firmware for your exact model (table, p. 5).
2. Change the admin password.
3. Replace every VPN key, WireGuard config and SSH key stored on the device, even if checks find nothing [6].

IF YOU SUSPECT ACCESS

1. Disconnect the device if it is safe to do so.
2. Flash firmware with "Keep Settings" off (router) or "Save current configuration" cleared (KVM).
3. Configure by hand with new credentials. Do not restore a backup from the device.
4. A factory reset alone does not apply the fixes [6].

KVM OWNERS: CHECK THE COMPUTER, NOT JUST THE BOX

A KVM sees the keyboard, screen and power of the machine attached to it. GL.iNet tells owners of affected KVMs to look on that computer for unfamiliar accounts, software, browser extensions, startup items and settings changes, and to run a full scan [6]. A community test found a startup script and SSH key survived a settings-preserving upgrade on an RM1 [7].

GL.iNet router · SSH (BusyBox) | root | READ-ONLY | NOT TESTED BY MAG212

community indicator check

```
ps w | grep -E 'crond -i /tmp/.log|mkfifo|
nc '
ls -la /tmp/f /tmp/.log 2>/dev/null
ls -la /bin/netstat
```

Looks for community-reported indicators: a crond started with /tmp/.log, a named pipe /tmp/f, and /bin/netstat that is not a symlink to busybox. Do NOT run netstat itself: GL.iNet staff warn a replaced netstat can start the malware [7]. Indicators are community-sourced; no output does not prove the device is clean. Not tested by MAG212.

NETWORK

- Watch and block 170.39.226.0/24 at the edge (community indicator) [7].
- Alert on routers opening outbound shells or long-lived connections to unknown hosts.
- Disable cloud management on devices you manage another way.

VERIFY RECOVERY

- Firmware version matches the table on p. 5.
- No unknown processes, cron entries or SSH keys.
- Old credentials no longer work anywhere they were used.

FOR MSPs AND IT MANAGERS

Small travel routers and IP-KVMs are often bought by individual staff and linked to a vendor cloud with a personal account. Ask who has them, especially KVMs on servers and admin workstations. A KVM in a server room is a remote hand on your most privileged keyboard. (MAG212 analysis)

PHP · CVE-2026-126714 · "phpAFTERSHELL"

phpAfterShell: one torn session file

October's PHP2Shell fix blocked one route into PHP's session handling. Researchers found the session file itself could still be turned against the server.

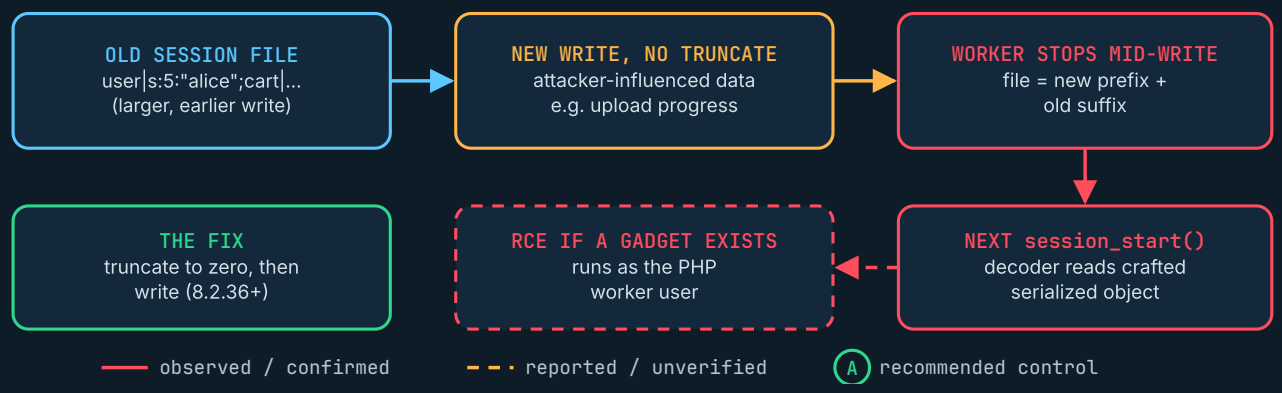


Figure 3 · How an interrupted session write becomes a deserialization, per PHP's advisory [9]. The final RCE step needs a gadget chain in the application, so it is dashed. MAG212 CYBER diagram.

WHAT HAPPENED

PHP's default `files` session handler writes new data over the old file without clearing it first. If the write is cut short, the file holds the start of the new session and the end of the old one, which can decode as attacker-chosen objects. Session upload progress lets a remote client shape that data. PHP rates it critical (CVSS 4.0 9.2) and says the code dates back to PHP 4.1.0. [9]

LINK TO PHP2SHELL

PHP2Shell (CVE-2026-109618/109619) was exploited in October. Its fix limited what the upload-progress callback could create but left the rewrite behaviour alone; Depthfirst's phpAfterShell research targets that gap. [10][11][12]

> **STATUS** Fixed 19 Nov. No in-the-wild attacks reported; public PoC writes only a harmless object; not in KEV [10, 12].

IF YOU CAN'T PATCH TODAY

- Set session.upload_progress.enabled = Off if unused.
- Store less untrusted data in sessions.
- Use a session store that replaces records atomically [9].

AFFECTED → FIXED

BRANCH	FIXED IN
8.2 and earlier	8.2.36
8.3	8.3.37
8.4	8.4.28
8.5	8.5.13

From GHSA-fm2m-fjf5-v3cp [9]. Older unsupported branches: upgrade.

Linux · shell | user | READ-ONLY

NOT TESTED BY MAG212

check one host

```
php -v
php -i | grep -E
'session.save_handler|upload_progress.
enabled'
```

Shows the version and session settings. Check PHP-FPM or the Apache module too; the CLI can differ. Not tested by MAG212.

AMAZON THREAT INTEL · CAIRN · MONAI LABEL · CVE-2026-133968

AI agents found a zero-day on their own, in about 11 minutes

Amazon watched a China-nexus actor point autonomous agents at university servers. They found and used an unknown flaw in a medical-imaging AI tool. CISA added it to KEV on 23 November.

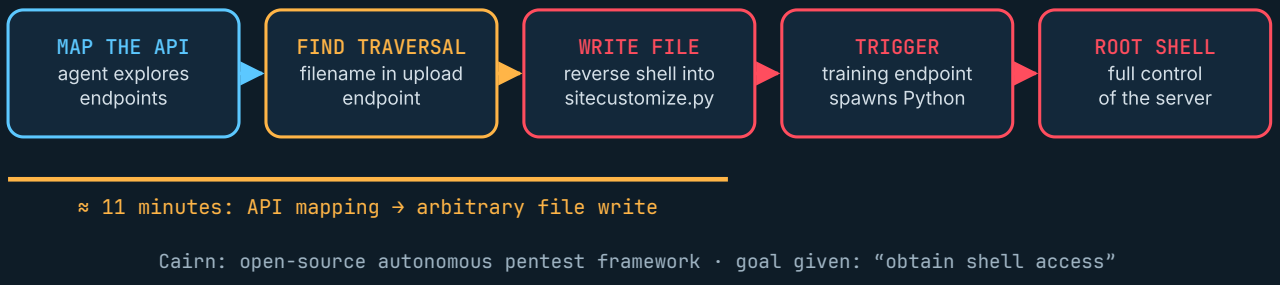


Figure 4 · The exploitation chain Amazon recovered from the actor's own exposed Cairn server [13]. MAG212 CYBER diagram.

WHAT HAPPENED

On 20 November Amazon's CISO CJ Moses described a campaign that began on 8 September. A Chinese-nexus actor (moderate confidence) gave agents built on Cairn, an open-source autonomous pentest framework, the goal "obtain shell access". Amazon found the actor's Cairn server exposed without authentication on 10 September, with its prompts and outputs visible. [13]

The agents found a path traversal in MONAI Label, an open-source medical-imaging AI tool, wrote a reverse shell into `sitecustomize.py` and got root. Amazon assesses with high confidence it was a zero-day. Other attempts failed: 16 hours and 148 actions against a Redis server, and more than 30,000 password guesses against a university GPU server and nearby systems. [13]

WHO IS AFFECTED

MONAI Label up to 0.8.5. Authentication is off by default. The flaw sits in `PUT /datastore/image` and `/datastore/label`. Version 0.8.6 was published on PyPI on 22 November. [14][15][16]

FIX AND CHECK

- Upgrade to `monailabel` 0.8.6; KEV due date 26 Nov [15, 16].
- Turn on authentication; never expose MONAI Label to the internet.
- Look for unexpected `sitecustomize.py` files in Python site-packages.
- Indicators from Amazon: 142[.]4.98.145 and 142[.]4.107.34 (seen 8–10 Sep) [13].

Linux · shell | user | READ-ONLY

NOT TESTED BY MAG212

check a MONAI Label host

```
pip show monailabel | grep Version
python3 -c 'import site;
print(site.getsitepackages())'
```

Compare the version with 0.8.6 and list the folders to search for an unexpected sitecustomize.py. Not tested by MAG212.

THE BIGGER LESSON

Agents work around the clock and at machine speed. Amazon's advice: let high-confidence detections trigger automatic response, with people supervising outcomes rather than approving every step [13].

Patch board: the shell week, sorted

The Hacker News called it “a whole lot of shell trouble”. Here is what is exploited, what only has a proof of concept, and what is still waiting for a release.

THE WEEK'S NAMED BUGS, AND WHERE THEY STAND ON 24 NOV

ITEM · CVE	WHAT	STATUS	ACTION
Java4Shell · CVE-2026-114938	OpenJDK x86-64 Base64 decoder; only AVX-512 VBMI/BW CPUs	NO ATTACKS · CHECK POC	OpenJDK 17 Nov updates for your JDK/vendor build
NGINX2Root · CVE-2026-123007 et al.	HTTP/2 bugs in NGINX and NGINX Plus	PUBLIC POC REPORTED	F5/nginx fixes; PAN-OS hotfixes or disable HTTP/2
Ruby2Shell · CVE-2026-132825	String case conversion heap overflow	NO ATTACKS · NO POC	Ruby 4.0.10 / 3.4.13 / 3.3.14
Ghostscript · CVE-2026-125396	Upload2Shell: crafted files reach a shell	NOT IN KEV	AlmaLinux fixed 23 Nov; RHEL fix pending
Tomcat · CVE-2026-133325	Cluster TLS-PSK peer not validated	FIX NOT RELEASED	11.0.30 still unreleased; use TLS 1.2
Idunno.AntiCsrf · CVE-2026-131914	Abandoned ASP.NET module, deserialization	EXPLOITED · NO PATCH	Find and remove it

Sources: [20–29]. Java4Shell and NGINX2Root were disclosed 17–20 Nov; listed here for status. Fixed versions for each JDK vendor differ: check your vendor.

CISA KEV: NEXT DEADLINES

CVE	PRODUCT	DUE
CVE-2026-124194	Microsoft Outlook	TODAY
CVE-2026-125350	Google Chromium	TODAY
CVE-2026-20320	Cisco BroadWorks	TODAY
CVE-2026-111793	Openwave Webtop	TODAY
CVE-2026-133968	MONAI Label	26 Nov
CVE-2026-134624	N-able Mail Assure	26 Nov
CVE-2026-115731	Puppet Enterprise	1 Dec
CVE-2026-40217	BerriAI LiteLLM	2 Dec

KEV v2026.11.23 (1,792 entries), checked 06:14 PT 24 Nov. Two additions on 23 Nov; none since [16].

PAN-OS: HOTFIX ETA PASSED

Palo Alto's advisory still showed an ETA of 23 Nov for 12.1.7-h15, 11.2.10-h19 and 11.2.13-h6 on 24 Nov, with no change-log update. Check the support portal; until then, disable HTTP/2 where it is on. Palo Alto is not aware of exploitation. [25]

GHOSTSCRIPT: DISTRO STATUS

- AlmaLinux 8/9/10: fixed packages in production on 23 Nov [27].
- RHEL: Red Hat bug still open, no fixed package [28].
- Debian 13 and Ubuntu fixed earlier; check your own tracker.

LAST WEEK'S KEV CLOSERS

vCenter, Cisco Expressway, Apache Roller and SAP NetWeaver were due 23 Nov. If any are still open, they are overdue: all four are exploited. [16][36]

Briefs

Shorter items and updates to stories we have covered this week.

OT · ENERGY

Cyber incident hits a US uranium mine

Peninsula Energy says its “operating system” at the Lance in-situ uranium project in Wyoming was breached and operations will be temporarily affected; US and Australian administrative systems were not. It halted ASX trading until 25 November. No attribution; ransomware is not mentioned. [30]

UPDATE · MSP

N-able Mail Assure flaw joins KEV

CISA added CVE-2026-134624, the SSRF N-able found while investigating the Mail Assure breach, to KEV on 23 November (due 26 November). N-able still has not said it was the way in; a root-cause report is promised within two weeks of 22 November. [16][18][19]

PAYMENTS

Cleverbridge: card numbers and CVVs copied

The reseller platform says a third party copied card numbers, expiry dates and CVV/CVC codes, found on 4 November; notices began 20 November. It has not said how many cards or which merchants' customers. Watch statements and replace affected cards. [31]

IDENTITY

Entra Connect Health: admins’ emails exposed

Microsoft says attackers read tenant metadata, including admin and technical contact emails, through a Connect Health flaw fixed on 19 November. No passwords or tokens were exposed. Expect targeted phishing of those addresses. [32]

AI SUPPLY CHAIN

Prompt-leak story: still no names

OpenRouter has not named the three inference providers it removed, and MiniMax has made no direct statement, as of 23 November. No new provider notices since Atlas Cloud's. Rotate secrets you ever sent in prompts through affected routes. [33][34]

PYPI · OLDER, 17–20 NOV

Microsoft’s agent-framework package was poisoned

Versions 1.26.1 and 1.26.2 of `agent-framework` on PyPI carried a credential stealer and are quarantined. Pin 1.26.0, rebuild from clean and rotate credentials from a clean machine if you installed them. [35]

ALSO TRACKED, NO NEW PRIMARY INFORMATION TODAY

- Webworm's rebuilt SoftEther VPN bridge (Rapid7, 19 Nov): The Hacker News covered it on 23 Nov; we found no new technical detail beyond Rapid7's report.
- Public-sector incidents (FBI NCIC, USDA): still no official statements on scope as of this morning.

Your work list for the week

Ordered by urgency. Each row points to the page with evidence and verification steps.

WHEN	TEAM	ACTION	SEE
TODAY	Cloud / IAM	Rotate all APIM Classic secrets, named values, IdP secrets and subscription keys	p.04
TODAY	Cloud	Check RuntimeVersion on every APIM gateway; contact Microsoft if below threshold	p.04
TODAY	Endpoint	Close KEV items due 24 Nov: Outlook, Chromium, BroadWorks, Openwave	p.09
48 H	Network / MSP	Update GL.iNet routers and KVMs; rebuild suspected devices without saved settings	p.06
48 H	Research / AI	Upgrade MONAI Label to 0.8.6 and turn on authentication (KEV due 26 Nov)	p.08
THIS WEEK	Web	Upgrade PHP to 8.2.36 / 8.3.37 / 8.4.28 / 8.5.13; disable upload progress if unused	p.07
THIS WEEK	Firewall	Apply PAN-OS hotfixes when available; until then disable HTTP/2	p.09
THIS WEEK	Identity	Warn admins whose emails Entra Connect Health exposed; enforce phishing-resistant MFA	p.10

ONE-PAGE HUNT SHEET

APIM	management writes, listSecrets, new subscriptions; old direct management API use
GL.iNet	crond -i /tmp/.log · /tmp/f · non-busybox /bin/netstat · 170.39.226.0/24 (community)
MONAI	unexpected sitecustomize.py · 142[.]4.98.145 · 142[.]4.107.34
PHP	corrupted or unusually large session files; worker crashes during uploads
Entra	phishing aimed at admin contacts in your tenant

BEFORE YOU CLOSE A TICKET

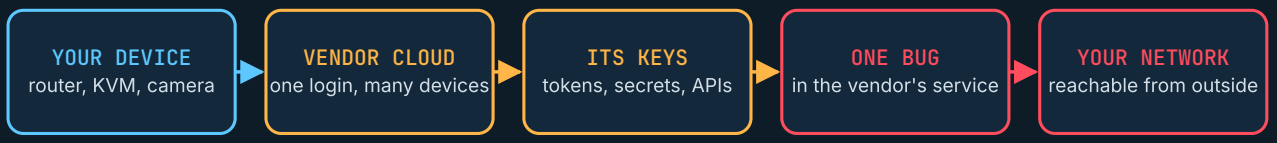
- Old APIM secrets fail when tested.
- Every gateway reports a patched RuntimeVersion.
- Device firmware matches the GL.iNet table; old keys revoked.
- php -v on the web SAPI, not just the CLI, shows a fixed build.
- pip show monailabel reports 0.8.6.

COMMAND SAFETY

Every command in this issue is read-only. They are generic checks built from vendor, NSM or researcher guidance. None was run by MAG212 for this issue; try them on one system first and adapt paths to your environment.

The cloud dashboard is a front door

A five-minute lesson for every employee, with notes for administrators and business leaders.



This week, two clouds held other people's keys: Azure API Management and GL.iNet GoodCloud.

Every convenience link is a door. Know which doors you have, and who holds the key.

Figure 5 · Why remote-management clouds matter, drawn from this week's APIM and GoodCloud incidents [1, 6]. Conceptual illustration, MAG212 CYBER.

FOR EVERY EMPLOYEE

- Don't plug a personal router, travel router or KVM into the office network without asking IT.
- If a device asks you to link it to a cloud account, ask IT first.
- Never paste passwords, keys or tokens into chats, tickets or AI tools.
- An email about “your admin account” or “tenant settings” deserves a second look this week.

FOR ADMINISTRATORS

- List every device and service with a vendor-cloud management link.
- Turn off cloud management where you manage another way.
- Keep secrets in a vault with owners and expiry dates, so you can rotate fast.
- Practise rotating one critical API key end to end.

FOR BUSINESS LEADERS

- Ask suppliers how they would tell you if their cloud exposed your keys, and how fast.
- Budget time for credential rotation; it is the only fix after a cloud-side leak.
- Make “who holds our keys?” a standing question in vendor reviews.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Which of our devices can be controlled from a vendor's website?
2. If a cloud provider leaked our API keys tonight, how long would rotation take?
3. Who would notice a router or KVM doing something new?

Sources

[1] Norwegian National Security Authority (NSM) · 20 Nov 2026, updated 23 Nov · NSM deler tiltak mot sårbarhet i Azure API Management

[2] SecurityWeek · 23 Nov 2026 · Azure flaw exploited to target secrets at Norwegian energy firms

[3] Anders Kristiansen · 21 Nov 2026 · Blog post on legacy direct management access in APIM

[4] Techzine · 24 Nov 2026 · Microsoft patches actively exploited vulnerability in Azure API Management

[5] Microsoft Tech Community · Nov 2026 · Rotating credentials in Azure API Management

[6] GL.iNet · 20 Nov 2026, updated 22–23 Nov · Security notice: GoodCloud remote management incident

[7] RemoteToHome (community) · 21 Nov 2026 · gl-security-incident-2026 analysis

[8] SecurityWeek · 23 Nov 2026 · GL.iNet routers, KVMs compromised via remote management service flaw

[9] PHP (php-src) · 19 Nov 2026 · GHSA-fm2m-fjf5-v3cp: Partially overwritten session files can lead to RCE (CVE-2026-126714)

[10] SecurityWeek · 23 Nov 2026 · phpAfterShell vulnerability revives PHP2Shell's attack path

[11] Depthfirst · Nov 2026 · phpAfterShell research

[12] SOCRadar · Nov 2026 · phpAfterShell CVE-2026-126714 and PHP2Shell

[13] AWS Security Blog (CJ Moses) · 20 Nov 2026 · Chinese-nexus actor's Cairn AI agents found a zero-day on their own

[14] Project MONAI · 18 Nov 2026 · GHSA-qc22-rmgc-vg94: MONAI Label path traversal

[15] PyPI · 22 Nov 2026 · monailabel release history (0.8.6)

[16] CISA · checked 24 Nov 2026, 06:14 PT · Known Exploited Vulnerabilities catalog (JSON v2026.11.23)

[17] Security Affairs · 24 Nov 2026 · CISA adds N-able MailAssure and Project MONAI flaws to KEV

[18] N-able · 22 Nov 2026 · Mail Assure incident update

[19] SecurityWeek · 23 Nov 2026 · N-able patches critical flaw discovered after Mail Assure cyberattack

[20] The Hacker News · 23 Nov 2026 · Weekly recap: VMware 0-day, Java4Shell, NGINX2Root, Ruby2Shell

[21] OpenJDK · 17 Nov 2026 · Vulnerability advisory 2026-11-17 (CVE-2026-114938)

[22] Help Net Security · 18 Nov 2026 · Java4Shell OpenJDK vulnerability CVE-2026-114938

[23] Ruby · 18 Nov 2026 · Multiple vulnerabilities in Regexp and String (CVE-2026-132825)

[24] SecurityWeek · Nov 2026 · F5 patches critical NGINX2Root flaws as PoC exploits go public

[25] Palo Alto Networks · 20–21 Nov 2026 · CVE-2026-123633: PAN-OS impact of nginx HTTP/2 vulnerabilities

[26] Apache Tomcat · checked 24 Nov 2026 · Fixed in Apache Tomcat 11.x (CVE-2026-133325)

[27] AlmaLinux · 22 Nov 2026, updated 23 Nov · Upload2Shell (CVE-2026-125396) fixes

[28] Red Hat Bugzilla · checked 24 Nov 2026 · Bug 2569593: CVE-2026-125396 ghostscript

[29] Mandiant · 18 Nov 2026 · MNDT-2026-0048: Idunno.AntiCsrf (CVE-2026-131914)

[30] SecurityWeek · 24 Nov 2026 · Peninsula Energy halts trading after cyber incident hits US uranium mine

[31] BleepingComputer · 22 Nov 2026 · Cleverbridge warns hackers stole credit card numbers, CVVs

[32] BleepingComputer · 21 Nov 2026 · Microsoft Entra Connect Health flaw exploited to steal tenant data

[33] OpenRouter · 22 Nov 2026 · Data processing incidents on inference providers

[34] Notebookcheck · 23 Nov 2026 · OpenRouter cuts three AI providers: who needs to rotate API keys now

[35] The Hacker News · Nov 2026 · Attackers compromise Microsoft's agent-framework PyPI package

[36] SecurityWeek · 23 Nov 2026 · SAP NetWeaver, Cisco Expressway flaws exploited in attacks

HOW WE VERIFIED THIS ISSUE

- Read directly: NSM's APIM notice, GL.iNet's security notice, PHP's GHSA-fm2m-fjf5-v3cp, Amazon's AWS Security Blog post, the CISA KEV JSON and PyPI's monailabel history.
- Microsoft's APIM customer notice was not available on a Microsoft page; its wording comes via SecurityWeek. GL.iNet device counts and the “nearly 200 routers” figure are from SecurityWeek and a community repo, not the vendor.
- Detection leads for APIM are from an independent researcher who says they may not match the actual vector. Webworm, NCIC and USDA had no new primary information.
- No command in this issue was executed by MAG212.

Read.
Verify.
Defend.

Free daily intelligence, CVE explainers and practical defensive guidance from MAG212 CYBER.

SUBSCRIBE FREE

Get every issue in your inbox

cyber.mag212.com/subscribe-free

MAG212 ATLAS · LIVE DEMO

Map every network before you test it

demo.atlas.mag212.com

WORK WITH MAG212 CYBER

Penetration testing
Find the forgotten edge before someone else does.

Network & security consulting
Inventory, segmentation and remote-access design.

Training
For staff, IT teams, leaders and schools.

cyber.mag212.com/services

Watch the Atlas walkthrough: youtu.be/j27B5g3viKw

MAG212 CYBER

Daily · 24 November 2026
Understand the threat. Build the defense.