

MAG212 CYBER

INTELLIGENCE • DEFENSE • TECHNOLOGY

WED 28 OCT 2026 • INTELLIGENCE EDITION

3

CVES SCORED
≥ 9.0 CRITICAL

2

ADDED TO CISA KEV
ON 27 OCT (REPORTED)

953

MAGENTO STORES IN
ONE LOADER CAMPAIGN

26,739

GMO CLOUD DESKTOPS
IN BREACH SCOPE

THE TRUST BOUNDARY ISSUE

WHEN TRUST BECOMES ACCESS

*Brotli. Tailscale. Magento. Oracle EBS. SkyW4lker. The technical paths
from exposure to control, verified against primary advisories.*

CVE-2026-111497

A decoder bug in every major Node.js line

CVE-2026-48356

PolyShell: patched stores, persistent loaders

CVE-2026-101767

Unauthenticated SQL to host on Oracle EBS

SKYW4LKER

Real Microsoft login, attacker-held tokens

EL MOSTAFA OUCHEN | MAG212 CYBER

Cover: AI-generated conceptual illustration. Not incident photography.

EDITORIAL

A sharper view of risk

BY EL MOSTAFA OUCHEN • CYBERSECURITY ADVISER • MAG212 CYBER

Security headlines arrive as names and numbers. Defenders need a different view: which component accepts untrusted input, which permission boundary fails, which assets are reachable, and what proves a fix is actually running.

This issue follows that chain across a JavaScript runtime, a private-network agent, a storefront database, an enterprise resource-planning suite and the Microsoft 365 sign-in itself. Then it moves from code to consequences: a Japanese hosting provider refusing a US\$50 million extortion demand, and the engineering reality behind quantum computing headlines.

Every story has been re-verified against vendor advisories, original research and the CISA Known Exploited Vulnerabilities (KEV) record as reported on 28 October 2026. Where sources disagree, we show both. Where we could not confirm a claim, we say so. A dedicated **verification ledger** on page 25 lists every correction made to our draft.

HOW TO READ THE CONFIDENCE LABELS

VERIFIED confirmed in a primary source (vendor, researcher, regulator). **REPORTED** attributed to secondary reporting; not independently confirmed. **EDITORIAL** MAG212 analysis or guidance; validate locally.

REPORTING WINDOW

Closes 28 October 2026, Pacific time. Advisories published earlier carry their own dates so a new headline is never mistaken for a new vulnerability. Live bulletins can change after press time.

IN THIS ISSUE

- 03

Threat dashboard
All CVEs, scores, KEV state
- 04

Nine days in October
Timeline, 20–28 Oct
- 05

Brotli / Node.js
The decoder boundary
- 07

Tailscale SSH
Authorized, then overprivileged
- 09

Magento / PolyShell
Malware beyond the filesystem
- 11

Oracle EBS
HTTP to database to host
- 13

SkyW4lker **NEW**
Device-code phishing, end to end
- 17

GMO Desktop Cloud
Extortion and recovery
- 19

Intel × Classiq
Owning the quantum stack
- 20

Post-quantum migration
Deadlines are now final
- 22

Technology radar
- 23

Detection engineering lab
- 24

The operator's 72-hour plan
- 25

Verification ledger
- 26

Sources, methods, glossary

PUBLICATION CREDITS

El Mostafa Ouchen
Cybersecurity Adviser, Editor
MAG212 CYBER
Publisher

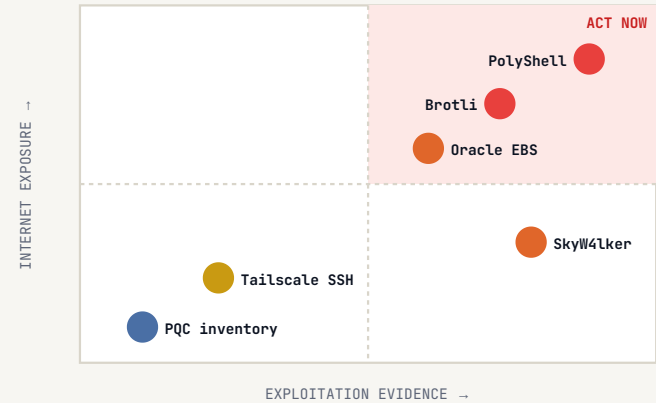
THE BRIEFING

Prioritize the reachable path

A vendor severity score describes a flaw. Your priority depends on exposure, exploitation evidence and what sits behind the component.

ISSUE	SCORE / VECTOR	CWE	EXPLOITATION	FIXED IN	PG
CVE-2026-111497 Node.js bundled Brotli decoder	9.2 v4 Google CNA 8.1 v3.1 Red Hat AV:N/AC:H/PR:N/UI:N	787, 252	KEV 27 Oct Due 10 Nov • honeypot attempts	22.23.4 24.22.1 26.12.1	05
TS-2026-014 ... 017 Tailscale SSH & Serve	No CVSS No CVE assigned	n/a	No in-the-wild reports; researcher PoC private	v1.104.4	07
CVE-2026-48356 "PolyShell" Adobe Commerce / Magento	9.6 bulletin 9.3 CVE record AV:N/AC:L/PR:N/UI:R/S:C	434	KEV 27 Oct (reported) Mass exploitation since Mar	APSB26-73 2.4.x-2026-jul	09
CVE-2026-101767 Oracle EBS • App Object Library	9.8 v3.1 Oracle AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	89 / 287, 306 disputed	Attempts since 22 Oct • not in KEV at press	Oct 2026 CPU (12.2.3-12.2.15)	11
SkyW4lker M365 device-code phishing kit	No CVE Protocol abuse	n/a	618 sandbox analyses Jun-21 Oct; MFA bypassed	CA: block device code fLow	13
GMO Desktop Cloud Hosted desktop breach	Incident	n/a	Credential theft, unauthorized FX trades	Service retired	17
NIST IR 8547 (final) PQC transition	Policy	n/a	Harvest-now, decrypt-later	ML-KEM / ML-DSA	20

EDITORIAL PRIORITY MATRIX



MAG212 editorial placement, not a measured risk score. Tailscale requires an authorized foothold; PQC is a planning horizon.

READ THE SCORES CAREFULLY

Three of this week's flaws carry **conflicting scores**. The Brotli flaw is 9.2 (CVSS v4, issuing CNA) but 8.1 at Red Hat because exploitation needs specific heap conditions (AC:H). Adobe's bulletin still shows 9.6 for PolyShell while the CVE record was rescored to 9.3 on 21 July (availability impact removed). Oracle does not call its flaw "SQL injection"; that label comes from Horizon3.ai.

BOTTOM LINE

Patch PolyShell and Brotli first where untrusted input reaches them: both are reported in KEV. Restrict /OA_HTML/AppsTcfServer today. In Microsoft 365, block device code flow with Conditional Access: no patch exists for SkyW4lker.

CHRONOLOGY

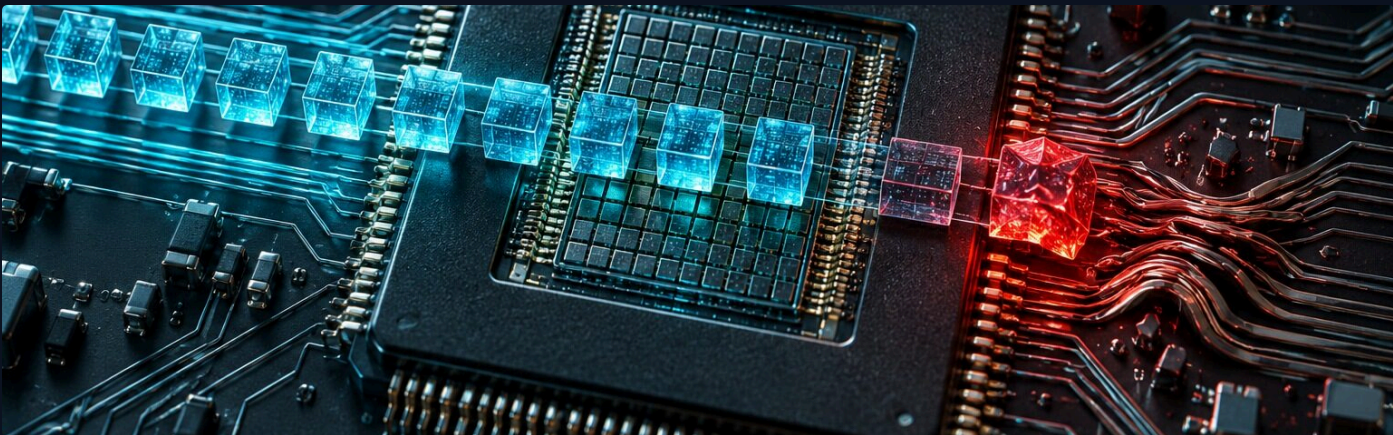
Nine days in October

Disclosure, patching, exploitation and extortion overlapped. The order matters for scoping incidents.

- 20 OCT**
- ORACLE** October CPU: 1,295 patches; CVE-2026-101767 (9.8) credited to Horizon3.ai.
 - GMO** Malicious programs found on Desktop Cloud customer servers.
- 21 OCT**
- NODE.JS** Security releases 22.23.4 / 24.22.1 / 26.12.1, fixing 10 CVEs incl. Brotli. Upstream Brotli 1.0.10 / 1.1.1 / 1.2.1.
 - GMO** 04:00 JST all plans shut down; ransom demand received; unauthorized FX trades begin.
- 22 OCT**
- NODE.JS** Public Brotli PoC: RCE only on weakened build; crash + leak on standard build.
 - ORACLE** First exploitation attempt on Previdian sensor, 17:28 UTC.
 - GMO** Police notified.
- 22-24**
- TAILSCALE** Researcher lab-tests 11 findings (“Tailworm”) vs v1.104.2 and headscale v0.29.5.
- 23 OCT**
- MAGENTO** Loader adds in-browser bot fingerprinting; patched 2.4.7-p10 store reinfected at 16:46 UTC.
- 24 OCT**
- MAGENTO** Sansec publishes deepveindrilling.com report: 953 stores.
 - TAILSCALE** Report received; publication follows within about two hours.
 - GMO** Customer data theft confirmed; ¥5,000 goodwill per user.
- 26 OCT**
- ORACLE** CPU revised (Rev 2); two unverified PoC repos appear.
 - TAILSCALE** Bulletins TS-2026-014 ... 017 dated.
 - INTEL** Agreement to acquire Classiq announced.
 - GMO** US\$50M demand disclosed by chairman.
- 27 OCT**
- CISA** Brotli flaw and PolyShell added to KEV (reported); Brotli due 10 Nov.
 - NIST** IR 8547 finalized.
 - ANY.RUN** SkyW4lker device-code phishing kit analysis published (618 analyses).
 - GMO** Attacker deadline passes; GMO refuses to pay.
- 28 OCT**
- TAILSCALE** “Findings and fixes”; v1.104.4.
 - GMO** US\$1M cybercrime bounty opens; attacker sites go offline ~04:00 JST.

Brotli: a small decoder, a large trust boundary

CVE-2026-111497. One mis-classified error code lets malformed compressed input write past an eight-byte buffer in native memory.



AI-generated editorial illustration: malformed input crosses a native-memory boundary.

WHAT IS CONFIRMED

VERIFIED

The Node.js advisory of 21 October states the root cause precisely: “An invalid block switch was reported as a temporary need for more input instead of a permanent format error, so the streaming decoder kept appending input bytes to an eight-byte internal buffer.” The decoder treated a fatal format error as “feed me more,” and each further chunk landed beyond the buffer.¹

The flaw is not Node-specific. It sits in Google's Brotli library: versions 1.0.3 through 1.2.0 are affected, fixed in 1.0.10, 1.1.1 and 1.2.1. Rapid7 and Red Hat list Bun, Python brotli/brotlicffi, .NET, Envoy/Istio, brotli4j, Firefox, Thunderbird and RHEL 7 through 10 among affected consumers.^{2,3}

HOW SERIOUS IS IT IN PRACTICE

REPORTED

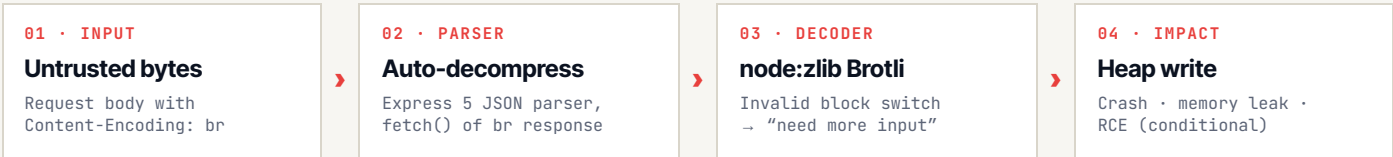
The public proof-of-concept released on 22 October reached code execution only on a deliberately weakened build; on standard builds it produced a crash and a limited memory leak. Red Hat's AC:H vector reflects that. CISA nevertheless added the flaw to KEV on 27 October with a 10 November deadline, shorter than its usual 21 days. Observed traffic is small: one Previdian sensor hit and one ELLIO-tracked source targeting Node 24.22.0, the last unpatched 24.x build.^{4,5}

THREAT CARD		KEV
CVE	CVE-2026-111497	
NICKNAME	“node2shell” (Red Hat RHSB-2026-015)	
CVSS V4	9.2 Critical • Google CNA	
CVSS V3.1	8.1 Important • Red Hat AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	
NODE.JS	High (no numeric score)	
CWE	787 out-of-bounds write • 252 unchecked return	
AFFECTED	Node 22.x, 24.x, 26.x • libbrotli 1.0.3-1.2.0	
FIXED	22.23.4 • 24.22.1 • 26.12.1 brotli 1.0.10 • 1.1.1 • 1.2.1	
EOL LINES	20.x and older: no fix	
KEV	Added 27 Oct • due 10 Nov	
CREDIT	OpenAI Codex Security (Khai Tran, Sylvie Mayer)	

[1] Node.js security releases, 21 Oct. [2] Red Hat CVE page & RHSB-2026-015. [3] Rapid7 ETR, 26 Oct. [4] The Hacker News, 28 Oct. [5] Previdian CVE page.

Find the decoder, then verify the process

Dependency presence and exploit reachability are different questions. Answer both.



MAG212 technical schematic. Conceptual sequence, not a captured attack trace.

REACHABLE ENTRY POINTS VERIFIED

PATH	WHO REPORTS IT
zlib.brotliDecompress(Sync)	Red Hat
zlib.createBrotliDecompress()	Red Hat
fetch() / undici decoding br	Red Hat, THN
Express 5 default body parsing	Sysdig via THN
WebSocket compression	UNVERIFIED

A server that only *sends* Brotli-compressed responses is not exposed by that operation. The vulnerable direction is **decoding** attacker-supplied bytes, inbound or from an untrusted upstream.

INVENTORY, INSIDE EACH RUNTIME

```
# run in every container / service context
node -p "process.version + ' brotli ' + process.versions.brotli"
node -p "process.config.variables.node_shared_brotli"
# if 'true': Node uses the OS library, patch it too
ldconfig -p | grep -i brotli
rpm -q libbrotli 2>/dev/null || dpkg -l 'libbrotli*'
```

Read-only. The shell's Node may differ from the binary a running worker uses. On Ubuntu 22.04+, RHEL 10, and Node 22 on RHEL 8/9, Node links the system Brotli.

TEMPORARY EXPOSURE REDUCTION EDITORIAL

Node.js publishes no workaround; upgrading is the only complete fix. Red Hat suggests rejecting or stripping Content-Encoding: br at the proxy for endpoints that do not need it:

```
# nginx: reject Brotli-encoded request bodies
if ($http_content_encoding ~* "br") {
    return 415;
}
```

Test against legitimate clients first. Vercel deployed equivalent inbound firewall rules on 21 Oct; they do not cover outbound fetch().

SAME RELEASE, NINE MORE CVEs

High: DNS NUL truncation (105482), TLS full-width digit IP (105483), loose TLS IP matching (106069). Medium: keep-alive (105481), non-canonical IPv4 certs (106072), randomUUID/randomInt entropy in snapshots & SEA (106074). Low: ZipFile (106070), Permission Model (106071, 106073). Compromised eMudhra intermediates were also distrusted.

VALIDATION GATE

Close the ticket when the **running** process reports a fixed version, base images are rebuilt by digest, every replica and long-lived worker has restarted, CI agents and bundled runtimes (Electron, SEA, Bun) are covered, and the OS libbrotli is updated where shared.

Tailscale SSH: identity is only one boundary

Four bulletins, one theme: a privileged daemon checked a path as text, then acted on it as root.



AI-generated illustration. The weak boundary sits inside an authorized connection, not in WireGuard cryptography.

BULLETIN	ISSUE	IMPACT	FIX IN 1.104.4
TS-2026-014	SSH Unix-socket forwarding validated paths lexically, then dialed as root. Three variants: ssh -L privileged dial, ssh -R unlink-and-replace of root sockets, allowlist race.	Reach Docker socket or tailscaled LocalAPI	Forwarding runs as the authenticated user
TS-2026-015	Window-change messages and env appends grow session memory without release.	OOM kill of tailscaled (DoS)	Bounded; freed on disconnect
TS-2026-016	Serve TCP forwards to Unix sockets dialed as root; symlink check only at config reload.	Full node takeover	TCP forwards limited; per-dial checks
TS-2026-017	HTTP/2 streams shared one serveHTTPContext under Serve TLS.	Tailscale-App-Capabilities leak across mounts	Per-request context

THE PRECONDITION VERIFIED

Tailscale's 28 October post says exploitation needs “an existing foothold on an authorized peer in the tailnet” with SSH permitted by policy. It frames the risk as lateral movement limited to connections the policy file allows. No CVE IDs or CVSS scores were assigned to any of the four bulletins.^{6,7}

THE “TAILWORM” DISPUTE REPORTED

Researcher Erica Windisch (Cyberdione Labs) published 11 findings against v1.104.2, headscale v0.29.5 and gliderssh, calling the chain “wormable”: sub-second hops, no credentials. Without Tailnet Lock, the lab chain captured an enrollment key and joined an attacker node; with Tailnet Lock that step failed. The PoC is private and unreproduced. She calls disclosure “reported but not coordinated”; Tailscale says it got the report on 24 Oct, about two hours before publication.⁸

02 / POLICY & HOST PRIVILEGE

Contain the path, not just the peer

Treat every SSH grant as a potential root-equivalent grant until the fleet runs 1.104.4.

01 • FOOTHOLD

Compromised peer

Already authorized
in the tailnet

02 • POLICY

SSH + forwarding

Grant allows
-L / -R forwarding

03 • DAEMON

Root dial

Lexical check,
root-context action

04 • HOST

Root socket

docker.sock,
LocalAPI → enroll

MAG212 technical schematic based on TS-2026-014 and researcher claims. Not a captured attack trace.

1 • DISABLE FORWARDING UNTIL PATCHED

```
# systemd drop-in (Linux)
sudo systemctl edit tailscaled
[Service]
Environment=TS_SSH_DISABLE_FORWARDING=1
sudo systemctl restart tailscaled
```

Vendor-documented mitigation for TS-2026-014. Keep an out-of-band recovery path before restarting remote hosts.

2 • VERIFY THE RUNNING VERSION

```
tailscale version
systemctl status tailscaled
journalctl -u tailscaled --since "2026-10-20"
```

Also check the admin console Machines list. Auto-update typically lags a release; do not assume coverage.

3 • NARROW THE SSH POLICY EDITORIAL

```
"ssh": [{
  "action": "check",
  "src": ["group:sre"],
  "dst": ["tag:prod"],
  "users": ["autogroup:nonroot"],
  "checkPeriod": "1h"
}]
```

Check mode re-authenticates people; it gates login, not the escalation itself. Tagged sources cannot use check mode.

WHAT TAILSCALE ACTUALLY RECOMMENDS VERIFIED

- ☐ Update all clients to v1.104.4 or later.
- ☐ Limit SSH policies to the users and devices that need them.
- ☐ Consider check mode for sensitive systems.
- ☐ VP Engineering: Tailscale is “not recommending that everyone disable Tailscale SSH.”

DEFENSE IN DEPTH EDITORIAL

- ☐ Enable **Tailnet Lock**: it blocked the final node-enrollment step in the researcher's lab.
- ☐ Remove Serve forwards to Unix sockets you do not need (TS-2026-016).
- ☐ Prefer per-pair grants over “any member to any tag.”
- ☐ Shorten node-key expiry on servers; review new enrollments daily this week.

HEADSCALE IS A SEPARATE PROJECT

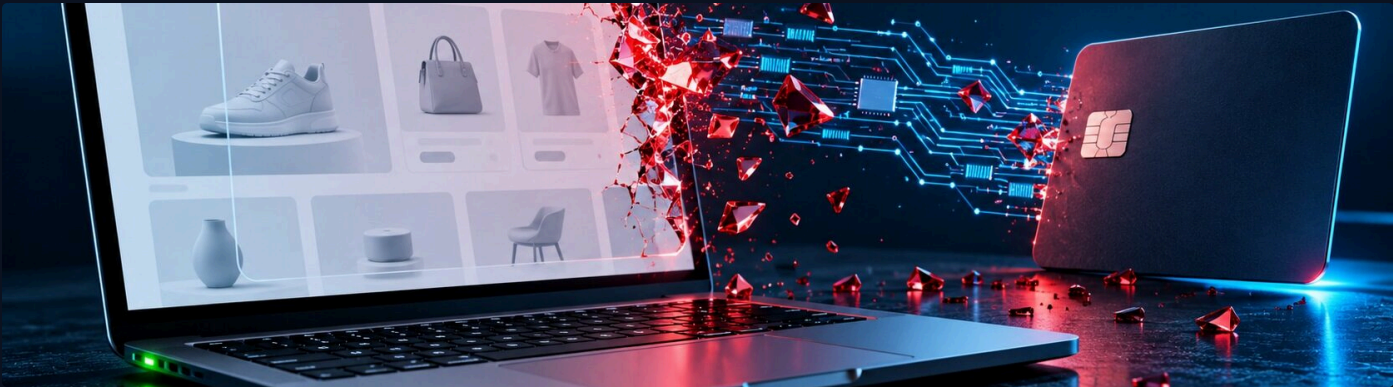
Upgrading clients to 1.104.4 addresses client-side bugs regardless of control server (our inference). But on headscale v0.29.5, SSH grants always include forwarding and policy cannot turn it off. Set the client variable. The researcher's headscale memory and registration-cache issues had no released fix at press time (PR #3586 pending).

AFTER UPDATING

Review unexpected node enrollment, policy edits and host activity since 20 Oct. If compromise is suspected, isolate the peer, delete it at the control plane, and rotate auth keys after preserving evidence.

The store is patched. Is the attacker still inside?

A 15-month loader campaign shows why a clean external scan and a current patch level are not closure.



AI-generated editorial illustration. No customer payment data or real storefront is depicted.

THE CAMPAIGN

VERIFIED

Sansec has tracked one operator across **953 stores** since 9 July 2025, mostly Magento. The newest domain, `deepveindrilling.com` (registered 6 Oct), sits in the CMS blocks of 83 stores, 60 of which already ran an earlier loader. The script lives only in the `cms_block` table: not in files, not in `core_config_data`.^[10]

The loader stores a payload under the `fpCode` key in the visitor's `localStorage` and replays it through an `onclick` handler, so it runs even when the domain is offline. Since 23 Oct it fingerprints browsers itself (`navigator.webdriver`, Selenium globals, `ChromeDriver.cdc_` properties), so automated scanners get a clean page. Sansec has **not captured the final payload**.

On 23 Oct a fully patched 2.4.7-p10 store received the loader one hour after a clean scan. A rogue admin (16 Sep) and a GSocket backdoor (24 Sep) had been found there earlier. **Patch state and eradication state are different facts.**

LOADER DOMAINS • STORES

<code>manulfie.click</code>	863
<code>neswnsssn.click</code>	494
<code>lanhd6549tdhse.top</code>	355
<code>additionalver.com</code>	246
<code>deepveindrilling.com</code>	83 • Oct 2026

Store counts overlap across domains. Source: Sansec, 24 Oct.

CVE-2026-48356 • POLYSHELL	
BULLETIN	APSB26-73 • 14 Jul • upd. 11 Aug
CVSS 3.1	9.6 Adobe • 9.3 CVE record
CWE	434 dangerous file upload
AUTH	None (guest cart REST API)
EXPLOITED	Since 19 Mar 2026
KEY	27 Oct (reported, unconfirmed)

[10] Sansec, “deepveindrilling.com: Magento CMS block loader hits 953 stores,” 24 Oct (mod. 25 Oct). [11] Adobe APSB26-73. [12] Sansec PolyShell research; Akamai, 27 Mar.

Hunt beyond the filesystem

Server persistence and browser execution are one incident. Scope both.

1 • DATABASE TRIAGE SANSEC QUERY

```
SELECT block_id, identifier, update_time
FROM   cms_block      -- repeat for cms_page
WHERE  content LIKE '%fpCode%'
OR     content LIKE '%se_referrer%'
OR     content LIKE '%localStorage.getItem%'
OR     content LIKE '%deepveindrilling%'
OR     content LIKE '%additionalver%';
```

Run on a read-only replica; adapt the table prefix. update_time marks the attacker's last write. Matches are leads: legitimate JS uses localStorage, and obfuscation defeats string search.

2 • POLYSHELL UPLOAD SWEEP

```
find pub/media/custom_options/ -type f ! -name '.htaccess'
find pub/media/customer_address/ -type f
find . -name 'accesson.php' -type f
# any .php / .html / .phar in upload dirs = strong IOC
```

3 • ACCOUNTS & PROCESSES

```
SELECT user_id, username, email, created, logdate
FROM   admin_user ORDER BY created DESC;
ps auxf | grep -iE 'gs-netcat|gsocket|defunct'
```

INDICATORS OF COMPROMISE VERIFIED

TYPE	VALUE
Loader	deepveindrilling[.]com
Loader	additionalver[.]com
Loader	lanhd6549tdhse[.]top
Loader*	manulfie[.]click · neswnsssn[.]click
Minor	hdfdsi84j3h[.]top · c85grt98sd[.]com
Payload	leqdger[.]click · crypto-insider[.]top
Storage	fpCode · 136c1e07507f4a97 · ...4a98
Decoy	Response body QWE=123;
Webshell	accesson.php · 780index.php · bypass.phtml · c.php · rce.php · json-shell.php

*Expired and re-registered May 2026 behind a parking service; still loaded on a handful of stores, so visitor data now reaches a new owner. Defanged with [.]

PATCH TO THE RIGHT BUILD

APSB26-73 affects Adobe Commerce 2.4.9, 2.4.8-p5, 2.4.7-p10, 2.4.6-p15, 2.4.5-p17, 2.4.4-p18 and earlier; Open Source 2.4.6-p15 to 2.4.9. Fixed builds use date names (e.g. 2.4.8-2026-jul). Sansec also advises APSB25-88 for SessionReaper (CVE-2025-54236).

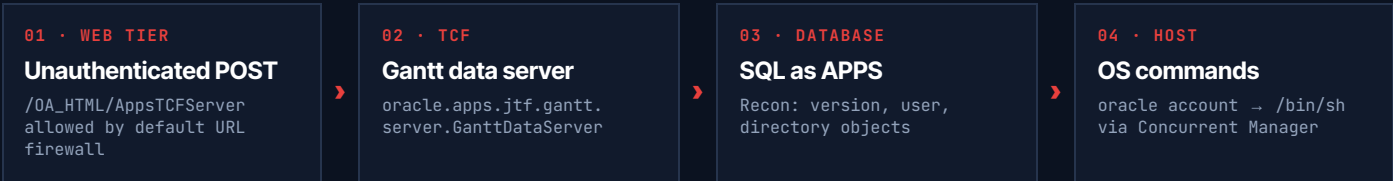
CLOSURE CHECKLIST

- ☐ Remove CMS scripts; restore blocks from trusted content.
- ☐ Close the entry point; delete webshells and rogue admins.
- ☐ Rotate DB, admin, API and integration secrets *after* containment.
- ☐ Deploy a CSP with reporting; alert on new script origins.
- ☐ Monitor cms_block.update_time for unexpected writes.

Sources [10]–[12]. Adobe's bulletin still says it is “not aware of any exploits in the wild”; Sansec documented mass exploitation from 19 Mar. No live malware was executed for this issue.

Oracle EBS: from HTTP to business data

CVE-2026-101767. A default-allowed servlet turns one unauthenticated request into SQL as APPS, and then into a shell.



Chain as described by Horizon3.ai, 20 Oct. No payload has been published by the researchers.

THE RESEARCHED CHAIN VERIFIED

Horizon3.ai identifies the TCF socket servlet (`oracle.apps.fnd.tcf.SocketServer`) at `/OA_HTML/AppsTcfServer` as the entry point. It describes unauthenticated SQL execution in the APPS schema and a chain to OS command execution as the EBS application account. Horizon3 reported it to Oracle on 24 July; Oracle credits Brandon Peterson, Jimi Sebree and Noah King.¹³

Impact follows the account's privileges: OS execution as the `oracle` user is not automatic root. But APPS can read finance, HR, procurement and payment records, which usually matter more than the host.

EXPLOITATION EVIDENCE REPORTED

Previdian logged the first attempt at 17:28 UTC on 22 Oct: 8 attempts from 5 IPs in 5 countries over seven days, six of them on 27 Oct, all on one sensor. Defused reported exploratory hits on EBS decoys on 27 Oct. Two public “PoC” repositories appeared on 26 Oct; both are unverified and may be malware. **Do not run them.** The CVE was not in KEV at press time.^{14,15}

WHY THIS ONE IS URGENT

EBS has been the target of mass extortion before: CVE-2025-61882 (9.8) was used in the 2025 Cl0p campaign against more than 100 organizations, and CVE-2026-46817 (Oracle Payments) was exploited in June 2026. Shadowserver counted about 950 internet-exposed EBS instances on 1 July.

THREAT CARD		9.8
CVE	CVE-2026-101767	
PRODUCT	EBS • Application Object Library • Core	
CVSS 3.1	9.8 Critical AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
CWE	89 + 306 (Horizon3) 287 + 306 (CVE trackers)	
AFFECTED	12.2.3 – 12.2.15	
FIXED	October 2026 CPU (20 Oct; Rev 2 26 Oct)	
AUTH	None	
KEV	Not listed at press	
PUBLIC POC	Unverified repos only	
CPU SCALE	1,295 patches • 95 critical CVEs (Tenable count)	

Oracle's advisory text does not use the words “SQL injection”; that characterization is Horizon3's.

[13] Horizon3.ai, CVE-2026-101767, 20 Oct; Oracle CPU Oct 2026. [14] Previdian CVE page. [15] SecurityWeek / Defused, 28 Oct.

A firewall is a path control, not a patch receipt

A validation plan for an ERP with multiple web tiers, load balancers and disaster-recovery nodes.

1 • ESTABLISH THE REAL ROUTE

Map load balancers, reverse proxies, origin addresses, partner links and DR nodes. An edge block is incomplete if a VPN partner or compromised workstation can still reach an origin.

2 • REMOVE THE SERVLET FROM THE ALLOWLIST

HORIZON3

Horizon3 recommends removing AppsTCFServer from the EBS URL firewall allowlist and restricting the web tier to trusted networks while patching.

```
# edge / reverse proxy: deny the TCF servlet
location ~* ^/OA_HTML/AppsTCFServer {
    deny all;
}
```

Validate dependencies first: legitimate features such as Gantt views may use TCF.

3 • PRESERVE BEFORE CLEANUP

Keep OHS/web access logs, proxy and WAF logs, database audit records and endpoint telemetry. Record clock offsets. On 12.2, collect OHS logs under the instance home (the 10.1.3 Apache path is R12.1-era). Do not delete files in \$APPLPTMP before responders image them.

4 • HUNT FOR HORIZON3'S INDICATORS

LAYER	LOOK FOR
Web	Unauthenticated POST to /OA_HTML/AppsTCFServer invoking GanttDataServer
Database	Recon soon after: v\$version, current user, all_directories
Filesystem	Unexpected files in \$APPLPTMP
Process	oracle spawning /bin/sh via Concurrent Manager

```
rg -n "AppsTCFServer" /path/to/exported-access.log
rg -n "POST .*AppsTCFServer" /path/to/*.log | \
  awk '{print $1}' | sort | uniq -c | sort -rn
```

Read-only search of an authorized export. A match is a lead, not a verified exploit; no match is not clearance if logs are incomplete.

5 • PROVE REMEDIATION

Record CPU patch IDs, the adop cycle result and service restarts. Retest every route with an approved non-destructive method (Horizon3 offers a NodeZero Rapid Response test). Keep the restriction until the owner accepts residual risk.

DECISION RECORD

asset owner + exposed route + CPU patch + adop cycle + verification result + evidence location + exception expiry

SkyW4lker: real Microsoft login, attacker-controlled authorization

A phishing kit that never needs a fake login page. The victim signs in on Microsoft's genuine site, passes MFA, and hands the session to someone else.

WHAT THE RESEARCH SHOWS VERIFIED

ANY.RUN's analysis of 27 October describes “**SkyW4lker x365 Sentinel**”, a Microsoft 365 phishing kit that abuses the OAuth 2.0 **device authorization grant**, the flow built for TVs and consoles that cannot show a full browser. ANY.RUN first saw it on 23 June 2026. Instead of stealing a password, it tricks the victim into approving a sign-in request the attacker started. The resulting tokens give access to whatever the account can reach: mail, files, Teams, and in many tenants the Microsoft Graph API. ANY.RUN notes the attack works even with MFA enabled.²⁶

WHY THE LOGIN LOOKS GENUINE

The victim types a short code into Microsoft's real device sign-in page (login.microsoftonline.com/common/oauth2/deviceauth), with a valid certificate on a Microsoft domain. Every visual cue a user is trained to check is correct. What's wrong is *whose device* is being authorized. Microsoft's login page is not compromised; this is **authorization deception**.²⁷

COUNT THE RIGHT THING VERIFIED

ANY.RUN counted **618 sandbox analyses** from June to 21 October 2026, rising from 20 a month in June to 200 in September. About 46–47% of submissions came from the US, then India, Canada and the UK. Submitting sectors were mainly technology, manufacturing and government (THN adds healthcare). These are **sandbox submissions, not confirmed victims**.

THE WIDER TREND

Device-code phishing is no longer niche. Microsoft tracked Storm-2372 using it from August 2024 (in July 2026 Microsoft linked that actor to Midnight Blizzard). Volexity documented Russian clusters in Feb 2025, Proofpoint reported a surge in Dec 2025, and the Tycoon2FA phishing service added it in May 2026.^{28,29}

THREAT CARD		ACTIVE
NAME	SkyW4lker x365 Sentinel	
TYPE	M365 OAuth device-code phishing kit	
FIRST SEEN	23 Jun 2026 (ANY.RUN)	
VOLUME	618 analyses to 21 Oct	
BYPASSES	Password theft not needed; MFA completed by victim	
BACKEND	Obfuscated JS + PHP, polling session API	
HOSTING	Miro, Google Sites, Zoom, Axure, Smartsheet, Cloudflare R2, Linode	
GATE	Cloudflare Turnstile or self-hosted CAPTCHA	
SIBLING	Gabagool kit, same developer (ANY.RUN, high confidence)	
CVE	None: abuses a legitimate protocol	
KEY FIX	Conditional Access: block device code flow	

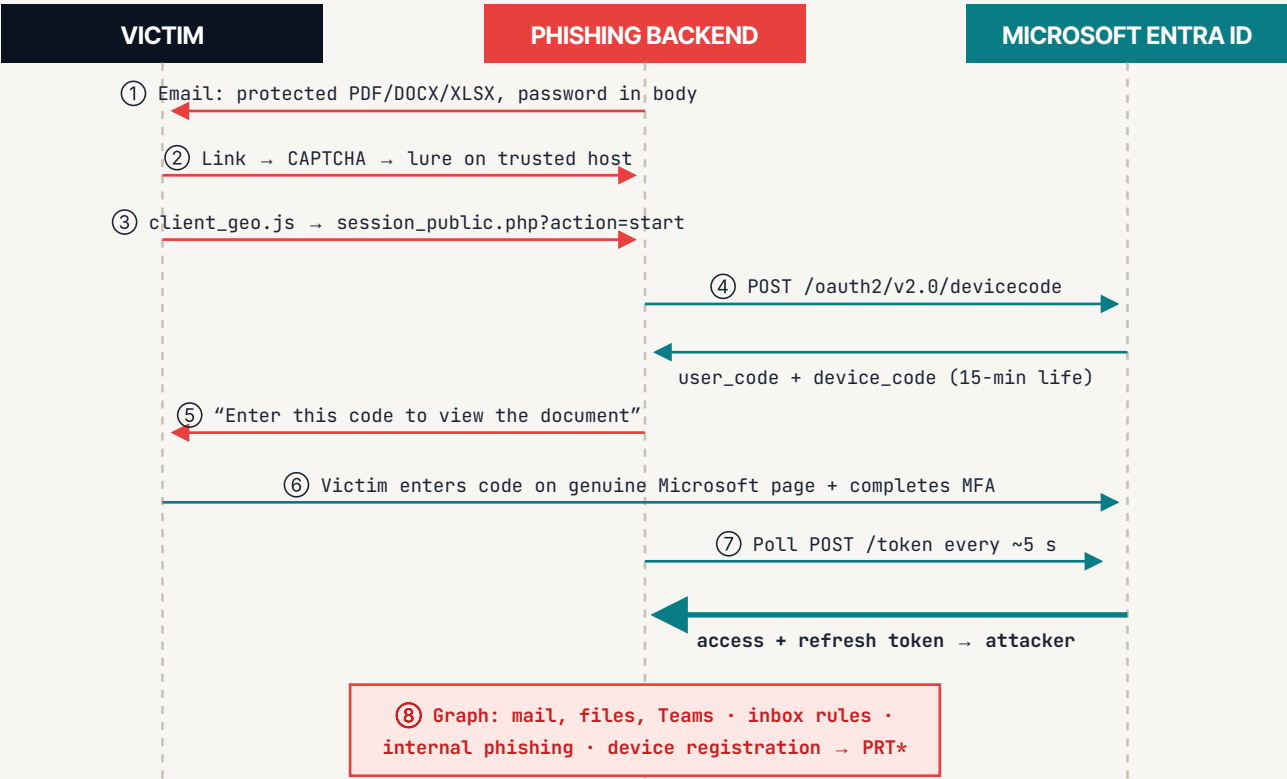
STAFF WARNING

Never enter a code from an email, document, chat or caller into a Microsoft page. Real IT requests never work that way.

[26] ANY.RUN, SkyW4lker phishing kit analysis, 27 Oct. [27] Microsoft Learn, OAuth 2.0 device authorization grant; RFC 8628. [28] Microsoft Threat Intelligence, Storm-2372. [29] Volexity; Proofpoint; BleepingComputer.

Anatomy of a device-code takeover

The attacker starts the sign-in, the victim finishes it, and Microsoft issues tokens to the party that started it.



MAG212 schematic from ANY.RUN (steps 1–3, 5), RFC 8628 and Microsoft Learn (4, 6–7), Microsoft/Volatility campaign reports (8). *Device registration was seen with Storm-2372; not confirmed for SkyW4lker. The client_id SkyW4lker requests is unpublished.

WHY MFA DOESN'T HELP

MFA proves the person at the keyboard is the user, and here they genuinely are. The authenticated state is then **transferred** to the device that requested the code. Phishing-resistant methods such as FIDO2 passkeys are satisfied too, because the victim uses them on the real Microsoft domain.

WHAT THE ATTACKER GETS

Access token	60–90 min (up to 28 h with CAE)
Refresh token	90-day inactivity window; renews on use
FOCI	“Family” refresh tokens can be redeemed for other Microsoft first-party apps

THE PRT ESCALATION

With the Microsoft Authentication Broker client (29d9ed98-...-f981bc1d605e), a refresh token can request the Device Registration Service, register an attacker device and obtain a **Primary Refresh Token**. That is a persistent, device-bound identity that survives password resets until the device is removed.

[26] ANY.RUN. [27] RFC 8628; Microsoft Learn token lifetimes & CAE. [28] Microsoft Storm-2372 (Feb 2025, upd. Jul 2026); Volatility, 13 Feb 2025; Secureworks FOCI research (Troopers 2022).

Find the code that someone else typed

Every device-code sign-in is labeled in Entra logs. Most users never need one, so a single hit is worth a look.

HUNT 1 • ALL DEVICE-CODE SIGN-INS (SENTINEL)

```
SigninLogs
| where TimeGenerated > ago(30d)
| where AuthenticationProtocol == "deviceCode"
| summarize Hits=count(), IPs=make_set(IPAddress),
  Apps=make_set(AppDisplayName),
  Risk=make_set(RiskLevelDuringSignIn)
  by UserPrincipalName, ResultType
| order by Hits desc
```

HUNT 2 • SESSIONS BORN FROM DEVICE CODE

```
SigninLogs
| where OriginalTransferMethod == "deviceCodeFlow"
| project TimeGenerated, UserPrincipalName, IPAddress,
  AppId, IncomingTokenType, UniqueTokenIdentifier
```

Refreshed sessions keep this marker, so it catches later token use from the attacker's infrastructure.

HUNT 3 • BROKER → DEVICE REGISTRATION

```
SigninLogs
| where AppId == "29d9ed98-a469-4536-ade2-f981bc1d605e"
| where ResourceIdentity ==
  "01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9"
| project TimeGenerated, UserPrincipalName, IPAddress,
  AuthenticationProtocol, IncomingTokenType
```

Authentication Broker requesting the Device Registration Service, the Storm-2372 PRT path. Confirm column names in your workspace.

SIGNALS THAT TURN A HIT INTO AN INCIDENT

- ☐ **IP mismatch:** MFA completed from the user's usual IP, token redeemed from a hosting provider or VPN minutes later.
- ☐ **Error 50199 then success** within about five minutes (Microsoft's Storm-2372 hunting logic).
- ☐ A user who has **never** used device code, on a laptop that doesn't need it.
- ☐ **New device registered** or new MFA method shortly after the sign-in.
- ☐ New **inbox rules** (delete, move to RSS/Archive), mass mail reads or internal phishing from the account.
- ☐ A click on a known lure host just before the sign-in (UrlClickEvents in Defender).

SCHEMA CHANGE

In Defender XDR advanced hunting, AADSignInEventsBeta was replaced by EntraIdSignInEvents on 19 Oct 2026, and the new table has no AuthenticationProtocol column. Use Sentinel SigninLogs or the Entra portal's "Authentication protocol: Device code" filter.

SKYW4LKER INDICATORS ANY.RUN

Paths	/assets/js/client_geo.js · /assets/js/endpoint.js · /assets/js/url_helper.js · /assets/php/endpoints/session_public.php · confirm_visit.php · /admin/index.php
Tokens	Landing regex it[A-Za-z0-9]{32}us (from 10 Aug)
Domains	173 listed, e.g. 5200m[.]com · torvion[.]life · ghethim[.]com · priorispace[.]biz · flow505.mooo[.]com
IPs	162.243.64[.]121 · 67.205.154[.]32 · 172.86.85[.]151 (shared with Gabagool)
Geo APIs	ip-api[.]com · ipapi[.]co · ipwho[.]is from lure pages

05 / REMEDIATION & PRECAUTIONS

Close the flow, then evict the session

A password reset alone does not end this attack. Tokens, sessions and registered devices must all go.

PREVENT • CONDITIONAL ACCESS MICROSOFT

1. **Audit first.** Run Hunt 1 for 30 days; list legitimate users (Teams Rooms, phones, panels, shared kiosks).
2. **Create the policy:** Users: All • Target resources: All • Conditions → **Authentication flows** → **Device code flow** • Grant: **Block**.
3. **Exclude narrowly:** a dedicated group of Teams resource accounts, ideally limited to named locations.
4. **Report-only for 1–2 weeks**, review impact, then switch to **On**.
5. **Add a second policy** blocking **Authentication transfer** (cross-device QR hand-off).

Blocked attempts return AADSTS530036. Protocol tracking also blocks later refreshes of a session that began with device code. Requires Entra ID P1. CIS M365 v6.0.1 control 5.2.2.12 calls for this block.

MICROSOFT-MANAGED POLICY

Many tenants already have a Microsoft-managed “Block device code flow” policy in Report-only. Microsoft switches it on after at least 30 days with two weeks' notice. Check yours now: when enforced, it has signed out non-excluded Teams Rooms on Android, phones and panels.

PRECAUTIONS FOR EVERYONE

- ☐ Treat password-protected attachments with the password in the body as suspicious.
- ☐ Restrict who can register or join devices to Entra ID.
- ☐ Require compliant devices for sensitive apps, so tokens on unmanaged attacker machines fail.
- ☐ Enable sign-in and user risk policies; keep Continuous Access Evaluation on.

RESPOND • EVICT THE ATTACKER

```
# Microsoft Graph PowerShell (Entra roles required)
$upn = "user@contoso.com"
Update-MgUser -UserId $upn -AccountEnabled:$false
Revoke-MgUserSignInSession -UserId $upn
# attacker-registered devices
Get-MgUserRegisteredDevice -UserId $upn
Update-MgDevice -DeviceId <id> -AccountEnabled:$false
# persistence review
Get-MgUserAuthenticationMethod -UserId $upn
Get-InboxRule -Mailbox $upn # Exchange Online
```

1. **Disable and revoke first.** Revocation invalidates refresh tokens; CAE-aware apps (Exchange, SharePoint, Teams, Graph) react within about 15 minutes. Other access tokens can last up to an hour.
2. **Remove devices** registered during the window; this kills any PRT.
3. **Reset the password** (twice in hybrid AD) and remove unknown MFA methods.
4. **Clean persistence:** inbox and forwarding rules, OAuth app consents, mailbox delegates.
5. **Scope the blast radius:** unified audit log for mail reads, file downloads and internal phishing from the account.
6. **Re-enable** only after the CA block is enforced for the user.

KNOW THE LIMITS

Token Protection binds tokens to the device they were issued to (GA for native Exchange, SharePoint and Teams apps on Windows, iOS and macOS). It cannot help if the attacker registered their own device and holds a PRT for it. **Phishing-resistant MFA** does not stop device-code phishing. Blocking the flow does.

[30] Microsoft Learn: Conditional Access authentication flows; managed policies; revoke user access; CAE; Token Protection (2026 revisions). CIS M365 Benchmark v6.0.1. Commands illustrative; test in your tenant.

GMO refuses to pay, and puts a price on attribution

A hosted trading-desktop breach becomes a test of customer protection, broker coordination and Japan's new cyber-defense law.



AI-generated conceptual illustration of account exposure. Not a reconstruction of the GMO incident.

WHAT HAPPENED REPORTED

GMO Internet found malicious programs on Onamae.com Desktop Cloud customer servers on 20 Oct and shut every plan down at 04:00 JST on 21 Oct. The service hosts Windows desktops that retail traders use to run MetaTrader 4/5 around the clock. MT4/MT5 logins stored on those desktops were stolen and used for unauthorized trades. OANDA Japan confirmed third-party logins; Japan's Finance Minister named five affected brokers.¹⁶

Up to **26,739 servers** are in scope. GMO stresses that this counts servers, not customers, and not confirmed intrusions. No card data was stored there. No group has been named and initial access is unconfirmed; the attackers claim a shared admin account.

THE COMPANY'S POSITION

The attackers demanded about US\$50 million, later reportedly cut to US\$1 million with a noon 27 Oct deadline. GMO refused. On 28 Oct it opened a **cybercrime bounty of up to US\$1 million in total**, paid only if a tip leads to an arrest or an international wanted notice, until 27 Oct 2027. Participants, buyers of leaked data and GMO staff are excluded.^{16,17}

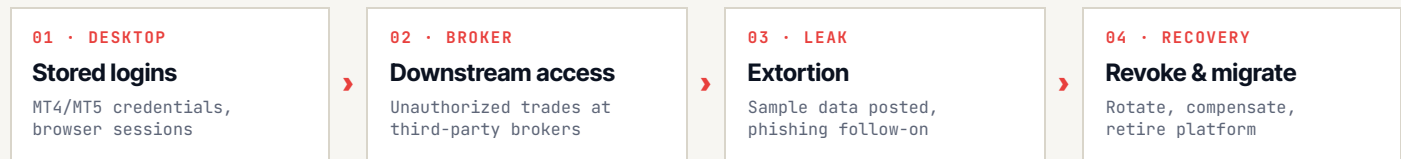
TWO US\$1M FIGURES, NOT ONE

The reduced ransom and the bounty share an amount but nothing else. The bounty is conditional, not an automatic payment for a tip.

[16] The Hacker News, 28 Oct; BleepingComputer; Impress Internet Watch. [17] GMO bounty terms as reported. GMO's own notice pages could not be loaded at press time.

Protect the downstream account

A hosted desktop concentrates credentials for other services. The breach does not end at the desktop.



MAG212 response model. Not a claim about GMO's internal architecture.

GMO'S REMEDIES REPORTED

- ☐ Compensation for losses from confirmed unauthorized trades.
- ☐ ¥10,000–25,000 per category of personal data confirmed published.
- ☐ ¥5,000 goodwill per user (announced 24 Oct).
- ☐ Platform will not restart; free six-month migration to another service.
- ☐ Official contact only from @cybercrimebounty.gmo; warns against paid “recovery” offers.

THE POLICY TEST

GMO asked the government to apply Japan's Active Cyber Defense law, in force since 1 Oct 2026. GMO is not a designated “Specified Social Infrastructure Operator,” and officials reportedly said the system is not triggered by individual company requests. Expect this case to shape how the law is applied.

LESSONS FOR ANY HOSTED-DESKTOP SERVICE

EDITORIAL

Credentials are a dependency

Map which downstream services each desktop could reach. Coordinate password changes with broker-side session revocation; a password reset alone may not end active sessions or API tokens.

No shared admin paths

If a shared administrative account is confirmed as the entry point, the lesson is per-tenant isolation, just-in-time admin credentials and phishing-resistant MFA on the management plane.

Separate three workstreams

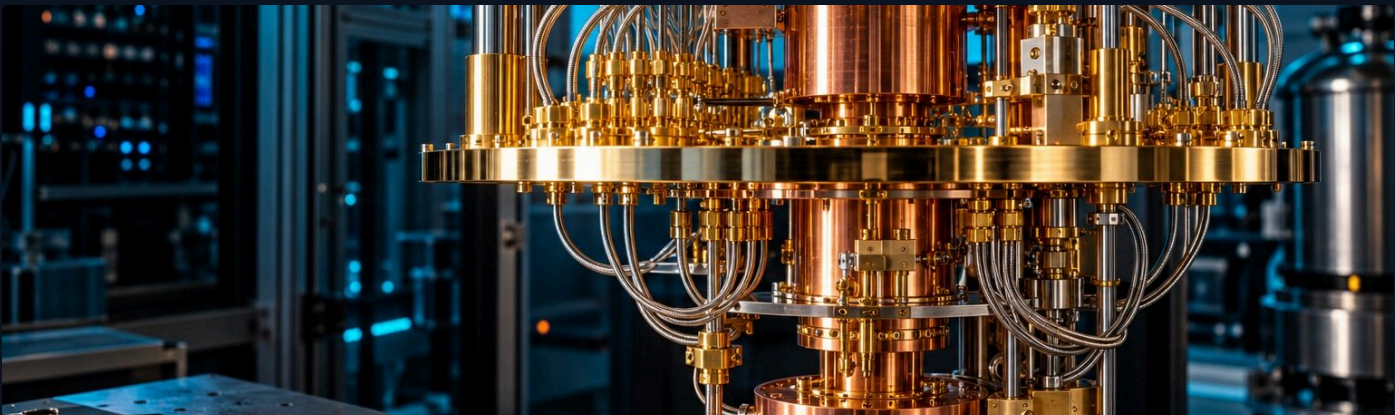
Containment keeps a trusted admin channel. **Recovery** restores from a verified state. **Investigation** preserves evidence and routes legal and law-enforcement contact through one incident owner.

MEASURE RECOVERY

Track confirmed affected identities, completed revocations, restored services and unresolved access paths. Never declare closure from uptime alone.

Intel's quantum bet: own more of the stack

The Classiq deal joins algorithm synthesis to silicon spin qubits. It does not bring cryptographically relevant quantum computing closer by itself.



AI-generated conceptual laboratory illustration. Not an Intel, Classiq or NIST facility.

THE ANNOUNCEMENT VERIFIED

On 26 Oct Intel announced an agreement to acquire Classiq, combining its quantum synthesis software with Intel's “scalable silicon spin-qubit technology.” Closing is expected in the first half of 2027, subject to regulatory approvals. Intel says it will keep Classiq's existing multi-platform integrations. Intel did not disclose a price; Bloomberg, Calcalist and Haaretz report about **US\$2.3 billion** in cash and shares.¹⁸

THE ENGINEERING QUESTION EDITORIAL

A full stack links a high-level problem to a circuit, a hardware target, a control system and measured results. Better synthesis uses scarce qubits more efficiently. It does not create fault tolerance. Intel CTO Pushkar Ranade called the deal “really a bet on the future.” Judge any future demonstration by reproducible workloads, logical-qubit counts, error rates and a classical baseline.

STACK SHEET

CLASSIQ	Founded 2020, Tel Aviv • ~130 staff • ~US\$200M raised (incl. US\$110M Series C, May 2025)
QUBIT CHIP	Tunnel Falls • 12 spin qubits (2023)
CONTROL	Horse Ridge II • 4 K cryo-CMOS
FAN-OUT	Pando Tree • 10–20 mK, up to 64 qubit terminals (2024)
FAB	Hillsboro, Oregon • “18AQ” process
CLOSE	H1 2027, subject to approvals

CONTEXT

Gidney (May 2025) estimates RSA-2048 falls to fewer than 1 million noisy qubits in under a week. Intel's published devices are in the tens of qubits.

[18] Intel Newsroom, 26 Oct; Bloomberg, Calcalist, SiliconANGLE. Deal value is reported, not disclosed.

The deadlines are now **final**

NIST finalized IR 8547 on 27 Oct 2026. Every quantum-vulnerable RSA and elliptic-curve algorithm is deprecated after 2030 and disallowed after 2035.

THE STANDARDS

VERIFIED

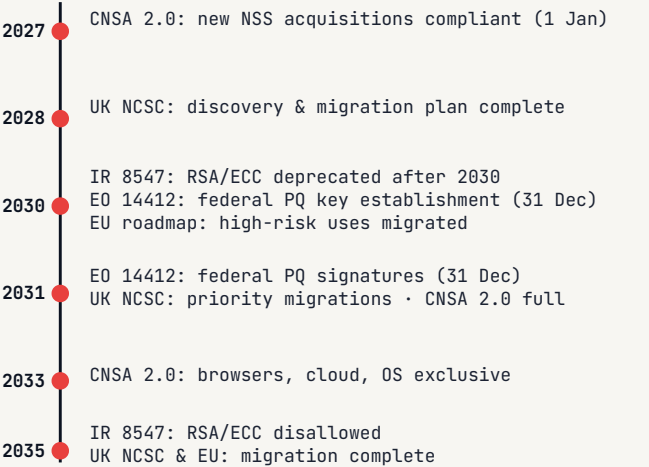
STANDARD	ALGORITHM	ROLE	STATUS
FIPS 203	ML-KEM	Key establishment	Final 13 Aug 2024
FIPS 204	ML-DSA	Signatures	Final 13 Aug 2024
FIPS 205	SLH-DSA	Hash-based sigs	Final 13 Aug 2024
FIPS 206	FN-DSA (Falcon)	Compact sigs	No public draft*
—	HQC	Backup KEM	Selected Mar 2025; final ~2027
SP 800-227	—	KEM guidance	Final Sep 2025

*Per a secondary tracker as of 20 Oct 2026; NIST page not reachable at press. Nine additional signature candidates entered Round 3 in May 2026.

KEY ESTABLISHMENT ≠ SIGNATURES

ML-KEM protects session keys against harvest-now, decrypt-later collection. ML-DSA protects authenticity: certificates, code signing, firmware. They migrate on different timelines and touch different systems. ML-KEM is not a drop-in label for every RSA use.

WHO MUST MOVE, AND WHEN



CNSA 2.0 dates from a secondary summary; EO 14412 signed 22 Jun 2026; NCSC milestones Mar 2025; EU roadmap Jun 2025.

FOR CONTRACTORS

EO 14412 also requires federal contractors to use FIPS-compliant post-quantum algorithms by 2030. That makes PQC a procurement question, not only a research topic.

Prepare for migration, not for a headline

Post-quantum cryptography runs on conventional systems. Much of it is already in your browser.

DEPLOYED TODAY

VERIFIED

PLATFORM	PQ CAPABILITY
Chrome / Edge 131+	X25519MLKEM768 default
Firefox desktop 132+	X25519MLKEM768 default
Safari 26 • iOS 26	Hybrid default in URLSession / Network
OpenSSL 3.5 (Apr 2025)	ML-KEM, ML-DSA, SLH-DSA; hybrid key share
OpenSSH 10.0	mlkem768x25519-sha256 default
OpenSSH 10.6 (6 Oct 2026)	Hybrid ML-DSA-44 + Ed25519 signatures
Windows	ML-KEM/ML-DSA in CNG; hybrid TLS opt-in*
iMessage • Signal	PQ3 (2024) • SPQR ratchet (2025)
Cloudflare	>50% of human traffic PQ (Apr 2026)

*Secondary source. Verify against Microsoft documentation for your build.

TEST YOUR OWN ENDPOINTS

```
# TLS: does the server negotiate hybrid ML-KEM?
(OpenSSL 3.5+)
openssl s_client -connect host:443 \
  -groups X25519MLKEM768 -brief </dev/null
# SSH: is PQ key exchange available and chosen?
ssh -Q kex | grep -i mlkem
ssh -v host 2>&1 | grep "kex: algorithm"
```

START WITH THE INVENTORY

EDITORIAL

Record algorithm, protocol, library, owner, data confidentiality lifetime, key custody, vendor support and upgrade constraints. Include certificates, VPNs, code-signing, HSMs, firmware roots of trust and archived sensitive traffic.

MAKE CHANGE TESTABLE

In a controlled pilot, measure handshake size, latency, CPU, memory, certificate-chain handling and middlebox compatibility. ML-KEM-768 adds about 1.1 KB to each side of the handshake, so watch for older load balancers that fragment or drop large ClientHello messages. Record failure modes and rollback criteria.

HYBRID IS A TRANSITION, NOT A PROOF

NIST's FAQ notes that hybrids add cost, performance effects and complexity and still need application-specific analysis. Combining two schemes is not a universal assurance argument.

SUPPLIER QUESTIONS FOR THIS QUARTER

☐

Which shipping release supports ML-KEM and ML-DSA, and is it FIPS-validated?

☐

How is downgrade to classical-only controlled and logged?

☐

What is the roadmap to meet IR 8547's 2030 deprecation?

THREAT HORIZON

Google (Mar 2026): under 500k qubits for 256-bit ECC. A Feb 2026 simulation-only claim puts RSA-2048 under 100k. Estimates keep falling; deployed hardware is far below them.

Infrastructure is strategy

Three developments behind the business headlines, and what each means for security teams.

AI HARDWARE / MALAYSIA VERIFIED

30 AI servers seized at KLIA

Malaysian customs intercepted 30 servers with advanced AI chips on 15 Oct in the free-trade zone at Kuala Lumpur's main airport, worth about RM50M (US\$12.2M). Falsely declared as electrical components, they were to be re-exported between two unnamed Asian countries without a permit. Customs links the group to five attempts, including 72 servers seized in June. Announced 28 Oct.²³

Implication: compute supply chains depend on provenance, transit controls and accurate declarations. Malaysia has required permits for transit of US-origin AI chips since 2025. Asset registers should record chain of custody, not just serial numbers. AP did not name the chip vendor.

AUTOMOTIVE / VOLKSWAGEN VERIFIED

China-developed architecture goes global

Reuters reports VW is shifting from “In China, for China” to exporting China-developed technology. The core is the Compact Main Platform with the China Electronic Architecture (CEA), co-developed with Xpeng in Hefei; Horizon Robotics is also a partner. The VEGA package (850 V charging, L3-ready) launches in 2027. Rollout starts in South America; Europe and North America are excluded for now.²⁴

Implication: examine software ownership, OTA update signing, regional key custody, telemetry routing and supplier SBOMs when a platform crosses markets. Connected-vehicle rules that restrict certain foreign software components shape where such platforms can ship.

AI ACCESS / INFISICAL VERIFIED

US\$40M to secure AI-agent access

Infisical raised a US\$40M Series B at a US\$600M valuation, led by Elad Gil with Gradient and Y Combinator (press release 27 Oct). Its new “Agent Vault” gives AI agents access to systems without handing them raw credentials, alongside secrets, PKI, KMS and privileged-access management. It claims 1,300+ customers, including Airbus, Volkswagen and Hugging Face.²⁵

Implication: agents need short-lived, task-scoped credentials, revocation and auditable tool use. Brokered access beats long-lived API keys in prompts or environment files. A funding round does not prove product efficacy; evaluate on your threat model.

[23] AP, 28 Oct. [24] Reuters, 28 Oct. [25] Infisical press release (PR Newswire), 27 Oct; SecurityWeek, 28 Oct.

PRACTICAL LAB / DETECTION

Turn a lead into evidence

Starting points for this week's threats. Untested in your environment: tune before you alert on them.

RULE 1 • ORACLE EBS TCF SERVLET ACCESS

```
title: Oracle EBS AppsTCFServer request (CVE-2026-101767)
status: experimental
logsource: { category: webserver }
detection:
  sel:
    cs-uri-stem|contains: '/OA_HTML/AppsTCFServer'
    cs-method: 'POST'
    filter_trusted:
      c-ip|cidr: '10.20.0.0/16' # your admin range
    condition: sel and not filter_trusted
level: high
```

RULE 2 • SHELL FROM THE EBS APPLICATION ACCOUNT

```
logsource: { product: linux, category: process_creation }
detection:
  sel:
    User: 'oracle'
    Image|endswith: ['/sh', '/bash', '/curl', '/wget']
    ParentImage|contains: ['FNDLIBR', 'java']
    condition: sel
```

Sigma-style. Concurrent Manager jobs legitimately spawn shells; baseline first and suppress with documented reasons.

RULE 3 • MAGENTO CMS-BLOCK WRITE OUTSIDE CHANGE WINDOW

```
SELECT block_id, identifier, update_time FROM cms_block
WHERE update_time > NOW() - INTERVAL 1 DAY
AND content REGEXP '<script|atob\\(|localStorage';
```

RULE 4 • BROTLI DECODER CRASH SIGNAL

```
// KQL-style: Node processes dying on memory faults
ContainerLog
| where LogEntry has_any ("SIGSEGV", "SIGABRT",
  "Segmentation fault", "free(): invalid")
| join kind=inner (Inventory
  | where NodeVersion !in
    ("22.23.4", "24.22.1", "26.12.1"))
  on ContainerID
| summarize crashes=count() by ContainerID,
  bin(TimeGenerated, 10m)
| where crashes >= 3
```

A crash loop on an unpatched runtime that accepts Content-Encoding: br is a lead worth triage. Pair with proxy logs for the request header.

RULE 5 • TAILSCALE ENROLLMENT AND POLICY DRIFT

Export admin-console audit logs (or stream them to your SIEM) and alert on: a new node joining outside provisioning automation; an ACL/policy change that adds SSH grants or forwarding; auth-key creation by an unexpected user. Correlate with tailscaled restarts or OOM events on servers (TS-2026-015).

A USEFUL EVENT RECORD

Identity	User, service account, device, auth context
Request	Time, method, normalized path, headers, status
Execution	Parent/child process, account, hash
Change	Deployment, policy, configuration revision
Evidence	Raw event location, retention, collection method

VALIDATION EXPERIMENT

Replay benign samples and approved safe test events in a lab. Measure coverage, false positives and missing fields before enabling alert-driven actions.

The next 72 hours

An adaptable response schedule for campus IT, systems teams and managed service providers.

WINDOW	NODE.JS / BROTLI	TAILSCALE	MAGENTO	ORACLE EBS	M365 / SKYW4LKER
00–04 h Identify & contain	Inventory running Node versions per service; check shared libbrotli; strip br at proxy where safe	Set TS_SSH_DISABLE_FORWARDING=1 on servers; list SSH grants	Run cms_block/cms_page query; sweep custom_options uploads	Deny /OA_HTML/AppsTCSFServer at edge; preserve web logs	Hunt deviceCode sign-ins; warn staff; block lure domains
04–24 h Patch & prove	Rebuild images on 22.23.4 / 24.22.1 / 26.12.1; restart workers; patch OS brotli	Roll v1.104.4 fleet-wide; verify via tailscale version and console	Apply APSB26-73 date build (and APSB25-88); audit admin_user	Apply Oct 2026 CPU via adop; record patch IDs and restart	CA block device code in report-only; scope exclusions
24–72 h Hunt & harden	Review crash loops since 21 Oct; cover CI agents, Electron, Bun, Python brotli	Audit enrollments since 20 Oct; enable Tailnet Lock; trim Serve socket forwards	Rotate secrets; deploy CSP reporting; monitor update_time	Hunt GanttDataServer requests, \$APPLPTMP files, oracle-spawned shells	Enforce block; revoke hits; remove rogue devices

DEADLINES TO TRACK

18 Nov 2026	CISA KEV due date, CVE-2026-111497 (federal civilian agencies)
27 Oct 2027	GMO bounty window closes (or on arrest)
H1 2027	Intel × Classiq expected close
1 Jan 2027	CNSA 2.0: new NSS acquisitions compliant
31 Dec 2030	Federal PQ key establishment (E0 14412)

KEEP THE HANDOFF CONCRETE

Every ticket carries the asset, owner, exposure condition, approved fix, verification evidence and next review date. For schools and smaller teams, protect administrative identities and recovery access first, and schedule changes around essential services.

ESCALATE SEPARATELY

Suspected compromise is an incident, not a patch task. Preserve evidence before cleanup and route it through your incident owner.

RESEARCH DESK / VERIFICATION LEDGER

What we checked, what we changed

Trust is earned in the corrections column. Every material change from our 28 October draft is listed here.

STORY	DRAFT SAID	NOW READS	BASIS
Brotli	Single severity implied	9.2 (v4, Google CNA) • 8.1 (v3.1, Red Hat) • High (Node.js), each attributed	[1][2]
Brotli	Node.js only	Upstream libbrotli 1.0.3-1.2.0 affected; OS library and other runtimes need patching	[2][3]
Brotli	“Honey-pot attack traffic”	Exploitation <i>attempts</i> : one Previdian hit, one ELLIO source. No confirmed compromise	[4][5]
Tailscale	Fix date unstated	Bulletins dated 26 Oct; v1.104.4 released around 27-28 Oct. No CVE or CVSS exists	[6][7]
Tailscale	Researcher unnamed	Erica Windisch, Cyberdione Labs; disclosure-timing dispute noted	[8]
Magento	“October loader ... 953 stores”	953 = whole campaign since Jul 2025; deepveindrilling.com on 83 stores	[10]
Magento	CVSS 9.6	9.6 in Adobe bulletin; CVE record rescored to 9.3 on 21 Jul	[11]
Magento	KEV not covered	Added 27 Oct per THN and Tenable; OpenCVE disagrees. Marked unconfirmed	[4]
Oracle	CWE not stated	CWE-89+306 (Horizon3) vs 287+306 (trackers); “SQL injection” attributed to Horizon3	[13]
Oracle	Exploitation “attempts”	Quantified: 8 attempts, 5 IPs, 5 countries, first 22 Oct 17:28 UTC; not in KEV	[14]
GMO	~US\$50M demand	Later reportedly cut to US\$1M; kept distinct from US\$1M bounty. 26,739 = servers, not customers	[16][17]
GMO	Notice No. 12, noon JST	Bounty opened 28 Oct (date confirmed); notice number and hour unconfirmed	[16]
Intel	Value not given	Undisclosed by Intel; reported ≈US\$2.3B (a US\$2.2B figure is unsupported)	[18]
PQC	NIST urges migration	IR 8547 final 27 Oct: all RSA/ECC deprecated after 2030, disallowed after 2035; EO 14412 deadlines added	[19][20]
SkyW4lker	“618 over six months”; code on microsoft.com page	618 sandbox analyses Jun-21 Oct (first seen 23 Jun), not victims; code entered on Microsoft's genuine device sign-in page	[26]
SkyW4lker	Microsoft recommends blocking	Plus Microsoft-managed block policy (report-only, auto-enforced after ≥30 days); not off by default	[30]
Radar	Infisical per SecurityWeek	Confirmed via company release (27 Oct); investors and product named	[25]

STILL OPEN AT PRESS TIME

KEV entries read first-hand (cisa.gov unreachable); PolyShell KEV status; upstream Brotli GHSA ID (two conflicting); FIPS 206 status from NIST directly; Tailscale per-rule forwarding toggle.

CORRECTIONS POLICY

Errors found after publication are corrected in the next edition with the original wording, the fix and the date. Readers can report issues to the editor.

RESEARCH DESK / REFERENCES

Primary sources & reporting

Numbered references match the article notes. Accessed 28 October 2026.

[1] NODE.JS PROJECT

October 2026 security releases, 21 Oct

nodejs.org/en/blog/vulnerability/october-2026-security-releases

[3] RAPID7

ETR: out-of-bounds write in Node.js Brotli decoder, 26 Oct

rapid7.com/blog/post/etr-cve-2026-111497...

[5] PREVIDIAN

CVE-2026-111497 sensor telemetry

previdian.com/CVE-2026-111497

[7] TAILSCALE

Security bulletins TS-2026-014 – 017

tailscale.com/security-bulletins

[9] TAILSCALE KB • THE HACKER NEWS

Tailscale SSH documentation; Unpatched Tailscale SSH flaws, 27 Oct

tailscale.com/kb/1193/tailscale-ssh

[11] ADOBE

APSB26-73, 14 Jul; updated 11 Aug 2026

adobe.com/trust/security/products/commerce/apsb26-73.html

[13] HORIZON3.AI • ORACLE

CVE-2026-101767 research, 20 Oct; Critical Patch Update October 2026

horizon3.ai/attack-research/vulnerabilities/cve-2026-101767 • oracle.com/security-alerts/cpuoct2026.html

[2] RED HAT

CVE-2026-111497; RHSB-2026-015 “node2shell,” 26 Oct

access.redhat.com/security/cve/CVE-2026-111497

[4] THE HACKER NEWS

PolyShell attacks breach hundreds of stores as Brotli exploit traffic emerges, 28 Oct

thehackernews.com/2026/10/adobe-commerce-polyshell-attacks-breach.html

[6] TAILSCALE

Tailscale SSH: Findings and fixes, 28 Oct

tailscale.com/blog/tailscale-ssh-findings-fixes

[8] CYBERDIONE LABS

Tailworm findings, updated 27 Oct

tailworm.com

[10] SANSEC FORENSICS TEAM

deepveindrilling.com: Magento CMS block loader hits 953 stores, 24 Oct

sansec.io/research/magento-cms-block-loader-deepveindrilling

[12] SANSEC • AKAMAI

PolyShell research; Magento PolyShell, 27 Mar

sansec.io/research/magento-polyshell

Evidence before certainty

[14] PREVIDIAN

CVE-2026-101767 exploitation-attempt telemetry
previdian.com/CVE-2026-101767

[16] THE HACKER NEWS • BLEEPINGCOMPUTER

GMO US\$1M bounty; Onamae Desktop Cloud hacked, up to 27,000 servers
thehackernews.com/2026/10/japans-gmo-offers-1-million-bounty-to.html

[18] INTEL NEWSROOM

Intel and Classiq, 26 Oct; Bloomberg deal reporting
intel.com/.../intel-classiq-accelerate-scalable-quantum-computing.html

[20] THE WHITE HOUSE

Executive Order 14412, 22 Jun 2026
whitehouse.gov/wp-content/uploads/2026/06/eo-14412.pdf

[22] GIDNEY • OPENSASH • CLOUDFLARE

arXiv 2505.15917; release notes; PQ support
arxiv.org/abs/2505.15917 • opensash.com/releasenotes.html

[24] REUTERS

Volkswagen to globalise China-developed technology, 28 Oct
ksl.com/article/51641888

[26] ANY.RUN • THE HACKER NEWS

SkyW4lker phishing kit analysis, 27 Oct; THN, 28 Oct
any.run/cybersecurity-blog/skyw4lker-phishing-kit-analysis

[28] MICROSOFT THREAT INTELLIGENCE

Storm-2372 device code phishing, Feb 2025 (upd. Jul 2026)
microsoft.com/en-us/security/blog/2025/02/13/storm-2372...

[30] MICROSOFT LEARN

Conditional Access authentication flows; revoke access; CAE
learn.microsoft.com/.../policy-block-authentication-flows

HOW THIS ISSUE WAS PRODUCED

Vendor advisories and original research anchor the technical features; news outlets supply attributed reporting. Every claim was re-checked on 28 Oct against at least one primary source where reachable. No original incident telemetry, interviews or lab exploit validation were obtained. Severity labels stay attributed to their publishers. Commands, rules and schematics are editorial material requiring local validation. Indicators are defanged.

Visuals: five AI-generated editorial artworks plus original vector schematics and charts. All are labeled; none is offered as a real incident photograph.

[15] SECURITYWEEK • BLEEPINGCOMPUTER

Oracle EBS flaw exploitation reporting, 28 Oct
bleepingcomputer.com/news/security/new-oracle-e-business-suite-flaw-now-exploited-in-attacks

[17] IMPRESS INTERNET WATCH • BUSINESS+IT

GMO incident coverage (Japanese)
internet.watch.impress.co.jp/docs/news/2150991.html

[19] NIST CSRC

IR 8547 (final); FIPS 203/204/205; PQC FAQ
csrc.nist.gov/pubs/ir/8547/final

[21] UK NCSC • EU

PQC migration timelines; EU coordinated roadmap
ncsc.gov.uk/guidance/pqc-migration-timelines

[23] ASSOCIATED PRESS

Malaysia seizes servers with advanced AI chips, 28 Oct
usnews.com/news/technology/articles/2026-10-28/malaysia-seizes-servers...

[25] INFISICAL

Raises US\$40M at US\$600M valuation, 27 Oct
prnewswire.com/news-releases/infisical-raises-40-million...

[27] IETF • MICROSOFT LEARN

RFC 8628; OAuth 2.0 device authorization grant
datatracker.ietf.org/doc/html/rfc8628

[29] VOLEXITY • PROOFPOINT

Device code phishing campaigns, Feb 2025; Dec 2025
vortexity.com/blog/2025/02/13/multiple-russian-threat-actors...

GLOSSARY

KEV	CISA Known Exploited Vulnerabilities catalog
CNA	CVE Numbering Authority issuing the ID
CWE	Common Weakness Enumeration category
CPU	Oracle quarterly Critical Patch Update
TCF	EBS Thin Client Framework servlet
LocalAPI	tailscaled's privileged control socket
ML-KEM	Module-lattice key encapsulation (FIPS 203)
CSP	Content Security Policy (browser)

MAG212 CYBER

*“Patch state and eradication state
are different facts.”*

Next edition: the November Patch Tuesday cycle, KEV follow-through on this week's flaws, and a field test of post-quantum TLS on legacy load balancers.

EDITOR

El Mostafa Ouchen

PUBLISHER

MAG212 CYBER

EDITION

28 October 2026

STANDARD

Verified · Reported · Editorial