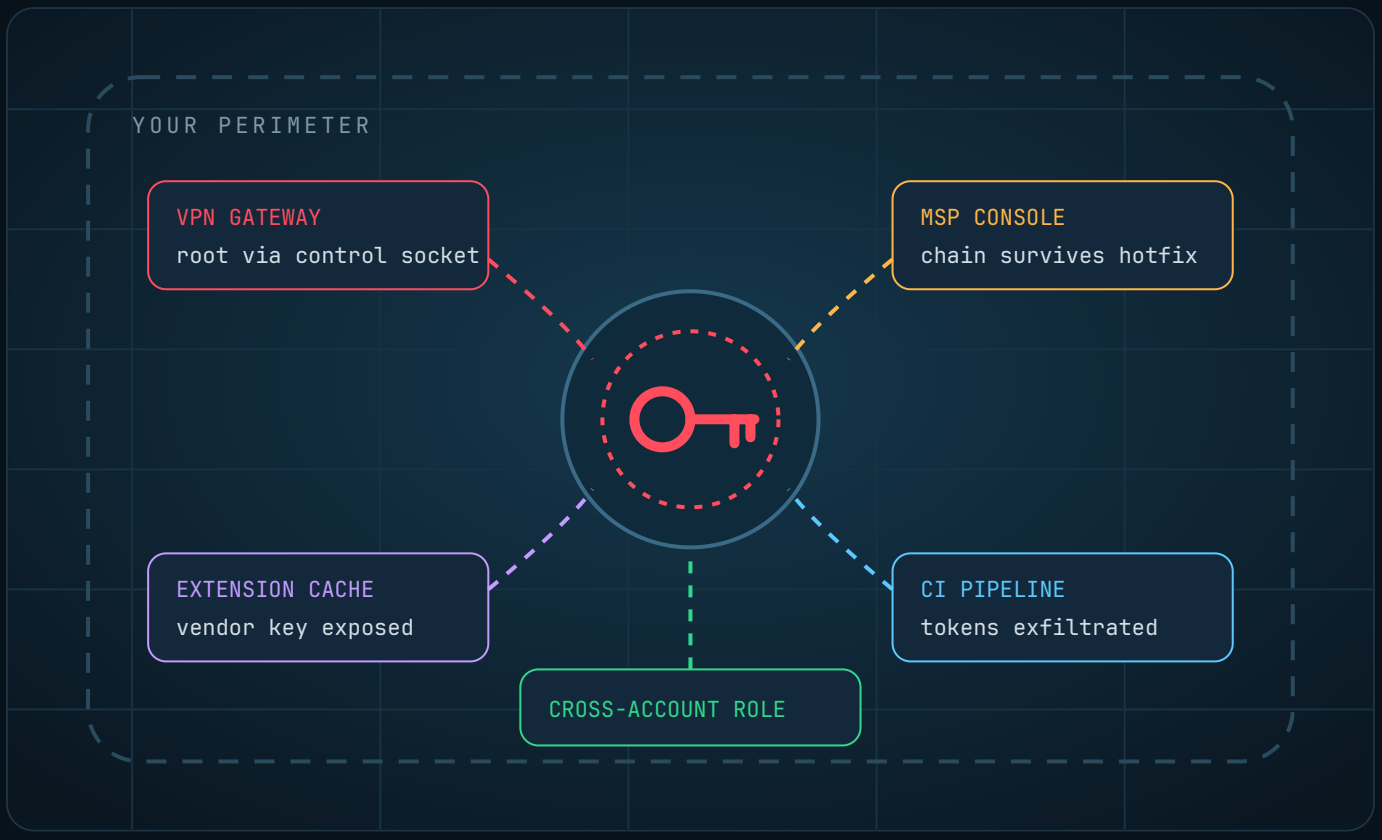
MAG212
CYBER

WEEKLY

Saturday, 14 November 2026

COVERING 8-14 NOV · CUTOFF 10:05 AM PST



WEEKLY CYBER INTELLIGENCE / NOV 8-14

The keys were already inside

Root on Check Point gateways, a second N-central chain that survives the hotfix, a vendor key that poisoned Cursor's marketplace, and thousands of GitHub accounts turned into CI secret stealers.

04 Check Point root exploit: hunt dynamicCli.log before Monday's KEV deadline

10 From Fireworks to Cursor to Notion: one AI vendor, three breaches

08 Outlook and Chrome zero-days, plus 12 KEV additions in five days

06 N-central after HF2: why the Legacy API decides your exposure

12 “wfx”: 4,800 hijacked GitHub accounts and the CI secrets they took

17 Not a hack: what really grounded US flights on Friday

EXECUTIVE BRIEFING · WEEK OF 8–14 NOVEMBER

What mattered this week

Vendor keys, management APIs, CI tokens and cross-account roles: the week's damage came through access defenders had already granted. Inventory and narrow those paths, not only patch.

EDGE & MANAGEMENT PLANES

Check Point confirms a Gaia root escalation in **dynamic_server** is exploited [3]; secondary reports add PHP2Shell entry and an ESXi wiper [6][7]. Barracuda confirmed ESG exploitation [11]. A new N-central chain bypasses HF2 where the Legacy API is exposed [9][10].

VENDOR-CUSTOMER TRUST

An exposed vendor key let an attacker plant malicious builds in Cursor's marketplace cache [26]. Notion: under 1% of workspaces had AI transcripts exposed via Fireworks [34][35]. Qubole identities assumed dormant roles in dozens of customer AWS accounts [40][41].

CLIENT ZERO-DAYS & THE PATCH WAVE

Microsoft (about 1,094 CVEs, 63 critical, by CSO's count) fixed the exploited Outlook CVE-2026-124194 [14]; Google fixed the exploited Chrome CVE-2026-125350 [20]. Fortinet, SAP, Adobe, PostgreSQL: big releases, no stated exploitation [14][59][62][64].

LAW ENFORCEMENT & ATTRIBUTION

Operation Endgame removed Gootloader from 100+ servers [47]. DOJ restrained $1.2 billion from the Binance theft and disrupted FaceStealer [51]. France attributed the refrigeration sabotage to an IRGC-linked unit [53]. Friday's FAA ground stop was **not** a cyberattack [77][78].

THE THREE HIGHEST-PRIORITY ACTIONS

1 Patch and hunt your edge and management planes today

- **Check Point:** run the sk1000362 log greps first to keep evidence, then install the fixed Jumbo Hotfix take on every gateway, management and log server. KEV due **Mon 16 Nov** [1][3]
- **Barracuda:** confirm patches, KEV was due **13 Nov** [1][11]. **N-central:** Legacy API off or unreachable, HF2, update Agents and Probes, hunt 13 Nov IoCs [10]

2 Hunt your developer and cloud trust paths

- Search GitHub for the wfx probe PR ("docs: dependency audit notes") and attacker branches from 10 Nov; CloudTrail for `CreateAccessKey` / `UpdateAssumeRolePolicy`; Entra ID for `wfx-ci-*` [36]
- Remove dormant third-party cross-account roles (Qubole, from 1 Oct) [40]. Act on Cursor, Notion, Apify or Railway notices by rotating named credentials from a clean device [26][35][44][68]

3 Close the exploited client bugs

- Push **Chrome 157.0.8103.50**+ and restart browsers [20]. Deploy the November Office update by channel for Outlook CVE-2026-124194, KEV due **24 Nov** [1][14]
- Upgrade and restart `sshd` on Alpine and other musl-based hosts without PAM (SSHole; KEV due 12 Nov, passed) [1][22]

CONTENTS

04 Check Point 06 N-central 07 Barracuda 08 Outlook & Chrome zero-days 09 SSHole
10 Cursor / Fireworks / Notion 12 "wfx" CI stealer 13 Cloud trust abuse 14 Gootloader & DOJ
15 Cold-chain & ICS 16 Patch briefs 17 Breaches, education, FAA, policy 18 KEV & patch board
19 Action desk 20 Awareness 21 Sources

WEEK AT A GLANCE · SUN 8 – SAT 14 NOVEMBER 2026

The week, day by day

CUTOFF 10:05 AM PST · Sat 14 Nov
18:05 UTC · America/Los_Angeles · last research note

KEV catalogVersion 2026.11.13
Released 2026-11-13 20:24 UTC · 12 CVEs added 9, 10, 13 Nov [1]

EDGE SUPPLY KEV PATCH BREACH LAW OPS

Times as published: UTC, ET, CET kept

SUN 8 NOV	EDGE	Check Point creates sk1000362: DynamicCLI root escalation, exploitation confirmed [3]
	SUPPLY	Unsigned `bee-worker` commit to bee-js (23:59:54 UTC) starts the npm compromise [38]
	BREACH	ESTT cloud ransomware; ~6.9 GB of claimed TSMC data offered for 3 BTC (claim only) [70][71]
	SUPPLY	Fireworks confirms to Notion that customer data was exposed [35]
MON 9 NOV	EDGE	~04:14 UTC: 33 N-central PoCs ("Able2Shell"); hosted N-central taken offline [9]
	SUPPLY	Malicious bee-js 13.3.0 is latest 00:09:50–01:24:58 UTC; Swarm Desktop 0.56.2 ~00:41–09:04 [38]
	PATCH	Chrome 157.0.8103.50/.51 fixes exploited CVE-2026-125350 [20]
	EDGE	Barracuda reports exploitation affecting "a small number of organizations" [11]
	KEV	+4: GPUStack, FreeSWITCH, OpenSSH "SSHole", IBM Aspera Faspex (due 12 Nov) [1]
	BREACH	Apify intrusion begins; Notion Fireworks advisory; Easthampton schools: no data stolen [35][68][82]
	LAW	France blames IRGC-linked SHAHID KAVEH for cold-chain sabotage; US advisory [52][53]
TUE 10 NOV	PATCH	Patch Tuesday: Microsoft (exploited Outlook CVE-2026-124194), SAP, Adobe, Fortinet (89 advisories), Siemens, Schneider [14][55][59][62]
	KEV	+6: Chrome, Outlook, BroadWorks, Openwave (due 24 Nov); two Barracuda (due 13 Nov) [1]
	EDGE	5:30 PM ET: N-central 2026.4 HF2 (build 2026.4.1.26) fixes seven CVEs [10]
	SUPPLY	wfx GitHub Actions stealer goes active; Qubole abuse disclosed; Railway report; Fireworks' second breach [31][36][40][44]
	BREACH	New Plymouth SD (ID) detects a "cyber threat"; ActiveCloud (Belarus) ransomware; Baker Tilly files with Texas AG; Node2Shell KEV due [56][71][74][81]
WED 11 NOV	BREACH	20:46 CET: Apify says it detected the intrusion and cut off access [68]
	BREACH	Maersk confirms theft from a legacy LF Logistics system; Arctic Wolf AntiFox findings; UK NCSC launches CyAS [45][69][83]
	BREACH	Richmond schools: data "may now be on the dark web"; New Plymouth cancels classes [80][81]
THU 12 NOV	EDGE	1:10 AM ET: 4EverAble2Shell, Agent2Shell; 6:30 AM ET: N-able cites Legacy API [10]
	EDGE	CVE-2026-123039 published; sk1000362 updated; wfx research; PostgreSQL: 52 CVEs [2][3][36][64]
	LAW	DOJ: Gootloader disrupted (Endgame); 100+ StealC servers dismantled; $1.2B Binance-theft funds restrained; FaceStealer disrupted [47][48][51]
	BREACH	TSMC tells SEC of breach via a cloud vendor; Apify names "a compromised credential" [68][70]
FRI 13 NOV	SUPPLY	Cursor root cause: the Fireworks-exposed key. 10:25 AM ET: N-able IoCs [10][26]
	KEV	+2: Check Point CVE-2026-123039, UnrealIRCd CVE-2026-114713 (due 16 Nov). Barracuda KEV deadline falls due [1]
	BREACH	UT Arlington confirms theft (Qilin claims it); ActiveCloud restores services; Apify moves to hash-only token storage [68][71][73]
	OPS	3:54 PM ET: FAA nationwide ground stop over ARTCC communication issues; airspace reopens 8:15 PM ET. Not a cyberattack, per the DHS Secretary [77][78]
SAT 14 NOV	OPS	About 700 Saturday flights already cancelled [78]
	OPS	Bloomberg: White House AI task force urges easier liability rules for AI incident disclosure. Research cutoff 10:05 AM PST [84]

EXPLOITED · VENDOR-CONFIRMED | CISA KEV · DUE MON 16 NOV | CVE-2026-123039 · CVSS 3.1 7.8

Root through the gateway

sk1000362 (created 8 Nov, modified 12 Nov): Check Point "observed an active exploit of this vulnerability against a couple of dozen customers" [3]. Local vector (AV:L/AC:L/PR:L) [2].

Status. Exploitation **confirmed by vendor** and in KEV. The entry chain and post-exploitation tooling are **reported by secondary sources citing Check Point Research**, which MAG212 could not reach [5][6][7]: from **30 Oct**, PHP2Shell on Mobile Access portals, then this escalation, webshells, the TSGA backdoor, TSProxy, and an ESXi pivot to deploy a wiper [6][7]. No public attribution. **Not to be confused with** Dream's 24 compromised firewalls in a PHP2Shell campaign: those are **Palo Alto Networks** devices [8].

WHO IS AFFECTED · PER sk1000362

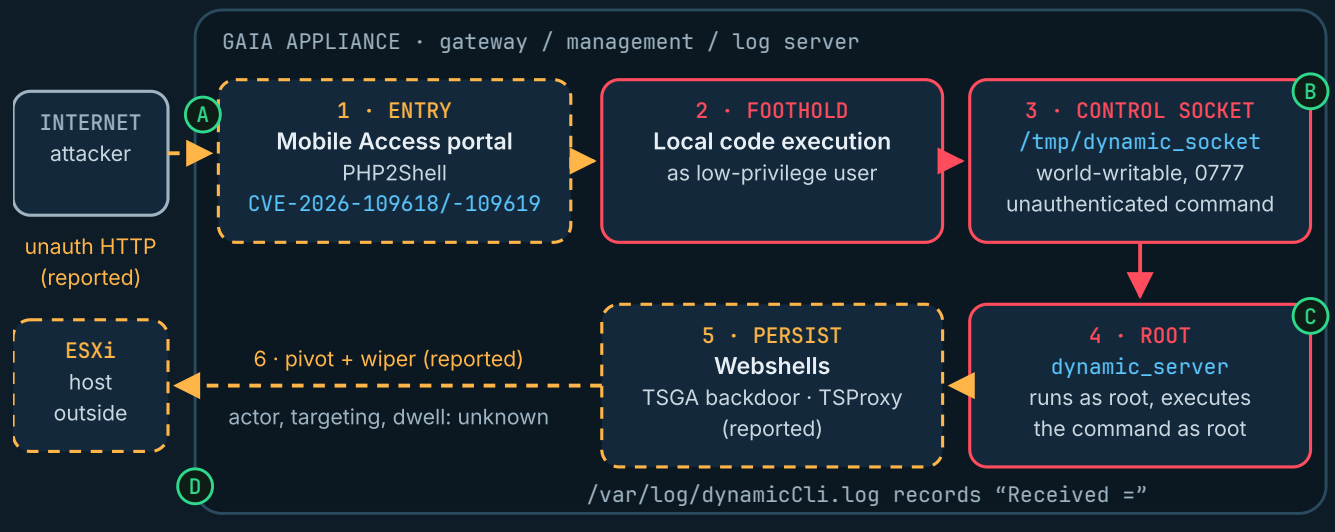
- **Affected:** Force Firewalls (Quantum Security Gateways); Management and Log Servers; Multi-Domain Security Management and Multi-Domain Log Server; Maestro Orchestrator
- **Not affected:** Spark Firewalls, Smart-1 Cloud
- **Releases:** R82.20, R82.10, R82, R81.20, R81.10, R81

Secondary coverage gives a wider "R80.30 to R82.20" scope; on R80.x, confirm with Check Point Support [6].

FIXED JUMBO HOTFIX TAKE

RELEASE	FIXED (sk1000362)
R82.20	Take 14+
R82.10	Take 52+
R82	Take 132+
R81.20	Take 174+
R81.10 / R81	No fix (EoS): upgrade

Conflict: the CVE record says R82.20 T10, R82.10 T50, R82 T130, R81.20 T173 "or below" [2]. Treat gap takes (R82.20 T11–13, R82.10 T51, R82 T131) as vulnerable.



A Restrict portal exposure; PHP2Shell fixed 21 Oct
B JHF fix: socket 0660 root:config
C Hunt with sk1000362 greps
D Ship appliance logs off-box
observed / vendor-confirmed — reported, not verified ○ recommended control

Diagram: MAG212 CYBER, based on [3][6][7]. How the attack works: steps 1, 5, 6 per secondary reports citing Check Point Research; steps 2–4 per sk1000362. PHP2Shell in KEV since 26 Oct [57].

Sources: [1] CISA KEV 2026.11.13 · [2] CVE record · [3] Check Point sk1000362 · [6] WindowsForum, 13 Nov · [7] CTO at NCSC digest · [8] The Record, 29 Oct

FEATURE 1 · CONTINUED · HUNT, CONTAIN, VERIFY

Hunt first, then patch

Copy `dynamicCli.log` and portal logs off-box **before** patching; run CP-1 to CP-3 on every member and server. The CVE needs a prior foothold, so hunt the entry vector too [3].

WHAT TO LOOK FOR · sk1000362

- Lines in `dynamicCli.log` without the Clish wrapper (CP-1) · `Received = #return_value#`, the uncommon `system()` sink
- Keywords: `id` `whoami` `/etc/shadow` `nc`/`ncat` `/dev/tcp` `curl` `wget` `base64` `useradd` `authorized_keys`. Admins may run curl or base64 legitimately: correlate with change tickets and admin sessions
- **Unverified, single-sourced leads:** `zz*.tpl` · `/tmp/CPconfigdaemon` · `/lib/libcpfwcommon.so` · `/opt/CPcvpn-R81.20/tmp/` · `130.94.19[.]204`

GAIA EXPERT MODE · grep | ADMIN | READ-ONLY | NOT TESTED BY MAG212

CP-1 / CP-2 · hunt (sk1000362)

```
grep "Received =" /var/log/dynamicCli.log | grep -vF "CPprofile.sh >> /dev/null; export
SP_DISTRIBUTE=0; set -o noglob;"
grep -F "Received = #return_value#" /var/log/dynamicCli.log
grep -EI "Received =.*( id;| whoami| /etc/shadow| ncat| nc -| /dev/tcp| curl | wget |
base64| useradd| authorized_keys)" /var/log/dynamicCli.log
```

CP-1 (first command): any output skipped the standard wrapper; review against admin activity. No output depends on log retention. **CP-2** (next two): a hit is high priority; correlate with admin sessions before declaring compromise.

GAIA EXPERT · CP-5 ALSO CLISH | ADMIN | READ-ONLY | NOT TESTED BY MAG212

CP-3b / CP-4 / CP-5 · verify (sk1000362, sk98028)

```
grep "Rejected connection from unauthorized uid" /var/log/dynamicCli.log
ls -l /tmp/dynamic_socket
ps auxw | grep -v grep | grep 'dynamic_server'
cpinfo -y all
show installer packages
```

CP-3b: a non-zero UID such as 99 (nobody) is an attempted escalation. **CP-4**: expect srw-rw---- root config (0660); 0777 is vulnerable; with the mitigation, no dynamic_server. **CP-5**: cpinfo (Expert, R81.x+) or Clish; compare with page 04 on every member [4].

CONTAIN & REMEDIATE · IN ORDER

01 Restrict portal exposure upstream
02 Preserve logs; install the fixed take [3]
03 Can't patch? Stop dynamic_server (sk **dbset** step)
04 Exploited? Rebuild; rotate secrets from a clean host
05 Upgrade R81.10 / R81 (no fix)

VERIFY · PREVENT

Confirm take and 0660 socket; test VPN auth and HA failover.

Prevent: keep management and Mobile Access off the internet; ship logs off-box; retire EoS releases; track PHP2Shell (fixed 21 Oct) [57].

Sources: [3] Check Point sk1000362 · [4] sk98028, JHF FAQ · [57] PHP2Shell. Commands copied from the sks.

VULNERABILITIES · VENDOR-CONFIRMED | EXPLOITATION · DISPUTED | NEW CHAINS: NO CVE, NO HF3

N-central after the hotfix

PoCs for 33 alleged flaws took hosted N-central offline on 9 Nov. HF2 fixed seven CVEs; then came a chain that beats HF2 wherever the non-default **Legacy API** is enabled and exposed [9][10].

EXPLOITATION STATUS IS IN CONFLICT

- **N-able:** scanning, but "no evidence that any customer environment had been successfully exploited"; none seen by Huntress [10]
- **watchTowr:** exploitation *attempts* on honeypots [9]
- N-able's own 13 Nov IoCs include **XMRig-delivery** infrastructure [10]
- Huntback's "live exploitation" claim (21 mining identities, 19 on HF2): **unverified**

WHAT HAPPENED

01 **9 Nov ~04:14 UTC:** 33 PoCs, no vendor notice; hosted offline, on-prem told to shut down. Censys: **1,728** reachable hosts [9]

02 **10 Nov 5:30 PM ET:** HF2, build 2026.4.1.26 [10]

03 **12 Nov 1:10 AM ET:** 4EverAble2Shell (root, beats HF2) and Agent2Shell (SYSTEM on endpoints); both need the Legacy API, N-able says [10]

FIXED IN HF2 · 10 NOV

CVE-2026-125883	XXE
CVE-2026-125878	OGNL injection
CVE-2026-125879	LPE to root via syslog-ng config
CVE-2026-125880	Stored XSS
CVE-2026-125881	SSRF
CVE-2026-125882	RCE via upload path traversal
CVE-2026-91000	Insecure IPC leading to LPE

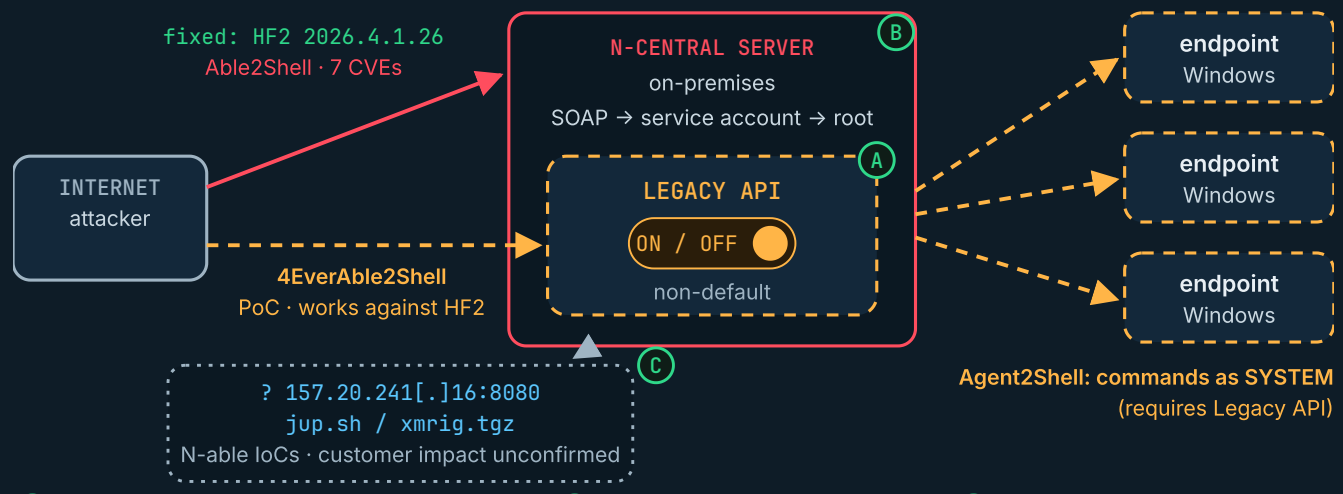


Diagram: MAG212 CYBER, based on [9][10]. Paths from published PoCs; RMM-channel abuse possible, not observed. Exploitation disputed: N-able reports scanning only; researchers report attempts.

LOOK FOR · N-ABLE IoCs, 13 NOV

hxxp://157.20.241[.]16:8080/jup.sh · /xvgz · /xmrig.tgz · /ob/fcheck · outbound 157.20.241[.]16 (8080, 19202–19418), 139.99.69[.]109:10128, 79.76.51[.]56:39100 [10]

Huntress, static only: SessionID −1 POSTs to /dms/services/ServerUI [10]

CONTAIN · IN ORDER

01 Legacy API off (N-able KB) or off the internet; **not** IP allowlisting alone [10]

02 Apply HF2; upgrade Agents and Probes too

03 Hunt IoCs; if compromised, rebuild, rotate RMM and customer credentials

Verify: version **may not change** [9]; confirm with N-able.

Sources: [9] CSA Labs, 10 Nov · [10] Huntress, 9–13 Nov · no verified N-able command doc

EXPLOITED · VENDOR-CONFIRMED | CISA KEV · DUE 13 NOV · PASSED | NO IOCs PUBLISHED

Barracuda ESG: internet to root in two flaws

Barracuda, 9 Nov: "We have identified exploitation activity affecting a small number of organizations." Two Mandiant-disclosed flaws chain to root; no attribution [11][12][13].

CVE-2026-116606 · CVSS 4.0 9.3

Pre-authentication authorization bypass (CWE-288). **ESG only**, versions before **9.4.0.030** [13]. Advisory published 2 Nov, updated 5 and 9 Nov [11].

CVE-2026-111560 · CVSS 4.0 8.6

Authenticated admin OS command injection via the timezone field, giving root (PR:H). ESG ≤ 9.4.0.27 · ADC ≤ 6.4.0 · WAF ≤ 11.0.1 · WSG ≤ 16.1.100.100 · BMA ≤ 5.5.4.0 · WCC ≤ 2.2.1 [12]

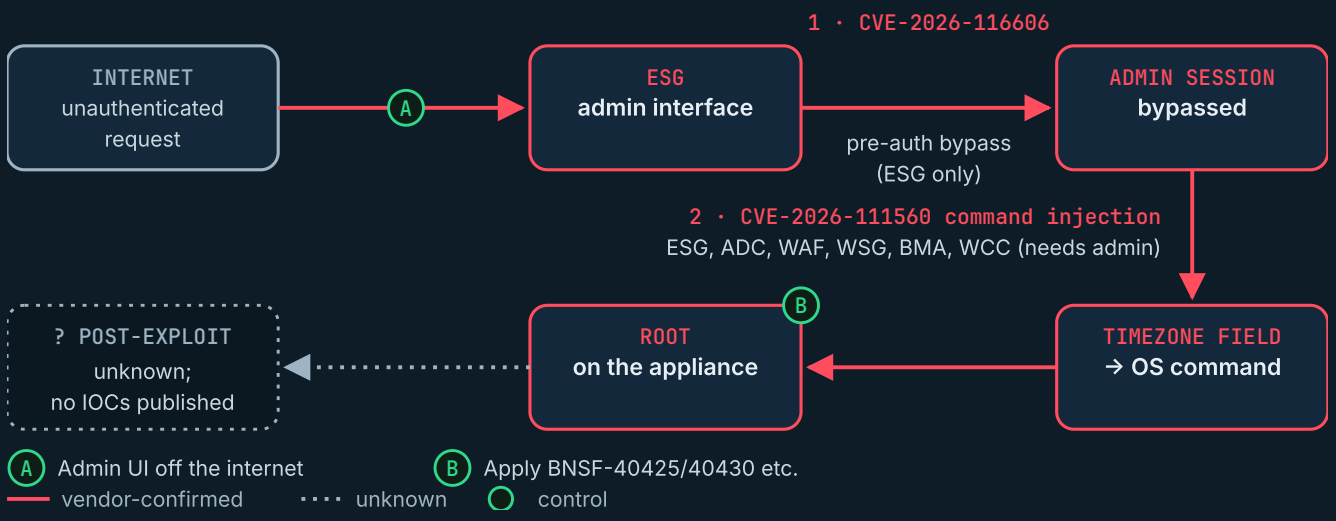


Diagram: MAG212 CYBER, based on [11][12][13]. On non-ESG products only step 2 applies, and it needs admin access. Unknown: post-exploitation, and whether every in-the-wild case used both steps.

PRODUCT	PATCH [11]	PRODUCT	PATCH [11]
ESG	BNSF-40425 (9.4.017 and later) / BNSF-40430 (before 9.4.017)	Load Balancer ADC	BNADC-16586
BMA	BNMA-32468	Web Comm. / WCC	BNWF-60060
WAF	BNADC-16586	Web Security GW (WSG)	BNYF-24789

LOOK FOR · MAG212 INFERENCE

Barracuda has published **no IOCs** [11]. Suggestions:

- Admin-interface sessions from unfamiliar IPs
- Unexpected timezone or config changes in the audit log
- Outbound connections to unusual hosts

Investigate: was the admin UI internet-reachable since 2 Nov? Export audit and system logs; call Barracuda support if exposed and unpatched.

CONTAIN & REMEDIATE · IN ORDER

01 Take admin interfaces off the internet (Barracuda's explicit guidance) [11]

02 Confirm the patch on each product

03 Exposed and unpatched? Treat as potentially compromised: rotate admin, mail-flow and LDAP secrets; rebuild with the vendor

Verify: patch ID on each appliance; admin UI unreachable from outside. **Prevent:** gateways hold directory credentials and see all mail: treat as tier-0.

Sources: [1] CISA KEV · [11] Barracuda advisory, 2/5/9 Nov · [12][13] Mandiant MNDT-2026-0041/-0042

OUTLOOK · EXPLOITED · KEV | CHROME · EXPLOITED · VENDOR-CONFIRMED | KEV DUE 24 NOV

Outlook leaks hashes, Chrome takes a zero-day

Microsoft fixed about **1,094 CVEs** (63 critical) [14][18]; the only exploited one leaks a user's **NTLMv2 hash**. Chrome patched an in-the-wild bug a day earlier.

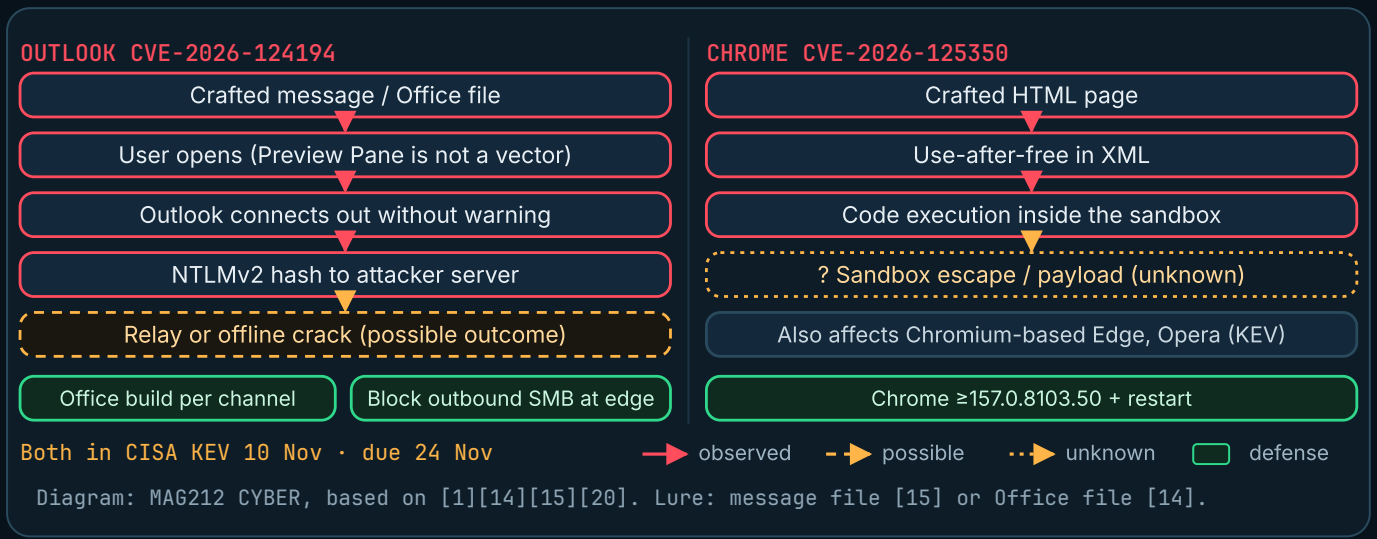


Diagram: MAG212 CYBER, based on [1][14][15][20]. Lure: message file [15] or Office file [14].

Outlook (CVSS 6.5): no external-content warning [14]; MSRC unreadable [16]; credit to "an Anthropic researcher using Claude" is single-sourced. **Chrome** (ADP 8.8): "Google is aware that an exploit for CVE-2026-125350 exists in the wild" [20]; "eighth" 2026 zero-day per Ivanti is **unverified** [14].

PRODUCT	FIXED VERSION / ROUTE
Office LTSC 2021 (Outlook)	16.0.14334.21048 [2]
Office LTSC 2024 (Outlook)	16.0.17932.21140 [2]
M365 Apps for Enterprise	aka.ms/OfficeSecurityReleases [2]. 10 Nov: Current 2610 (20527.20196) · Monthly Ent. 2610 (20527.20194), 2609 (20430.20264), 2608 (20326.20320) · Semi-Annual Ent. 2610 (20527.20192), 2609 (20430.20262), 2608 (20326.20318). Not labelled as carrying this fix [17]
Chrome · Edge, Opera	157.0.8103.50/.51 (Win/Mac), 157.0.8103.50 (Linux) [20] · Edge, Opera affected per KEV: apply vendor update [1]

WHAT TO LOOK FOR

- External attachment **then a file-open event**
- Outlook connecting to non-mail, non-Microsoft hosts
- Outbound auth to the internet; SMB 445/WebDAV (**MAG212 inference**)
- Chrome crashes clustered on one site
- **FP:** legitimate .msg workflows

CONTAIN & REMEDIATE · IN ORDER

1. Office security update, per channel
2. Update Chrome, Edge, Opera; force restart
3. Block outbound SMB to the internet (MAG212)
4. If exposed: reset password, revoke sessions
5. CVSS 9.8s: **CVE-2026-119958** LDAP, **-118207** Exchange [14]

Verify: Click-to-Run updates are **not** Windows hotfixes, so check each Outlook build per channel (MAG212, from [17]). **Prevent:** verify unexpected message files via a known channel; restrict NTLM after staging tests.

Sources: [1] CISA KEV 2026.11.13 · [2] cvelistV5 · [14] CSO 10 Nov · [15] eSecurityPlanet 11 Nov · [17] MS Learn M365 Apps history · [20] Chrome Releases 9 Nov

FIX VENDOR-CONFIRMED | EXPLOITED PER CISA KEV | KEV DUE 12 NOV · PASSED | CVSS 8.1

SSHole: a narrow OpenSSH bypass in KEV

On musl systems with PAM off, sshd misreads a string as a password hash: “any password between 256 and 1024 characters succeeds” [2]. Fixed in **10.6p2** (5 Nov) [21][24].

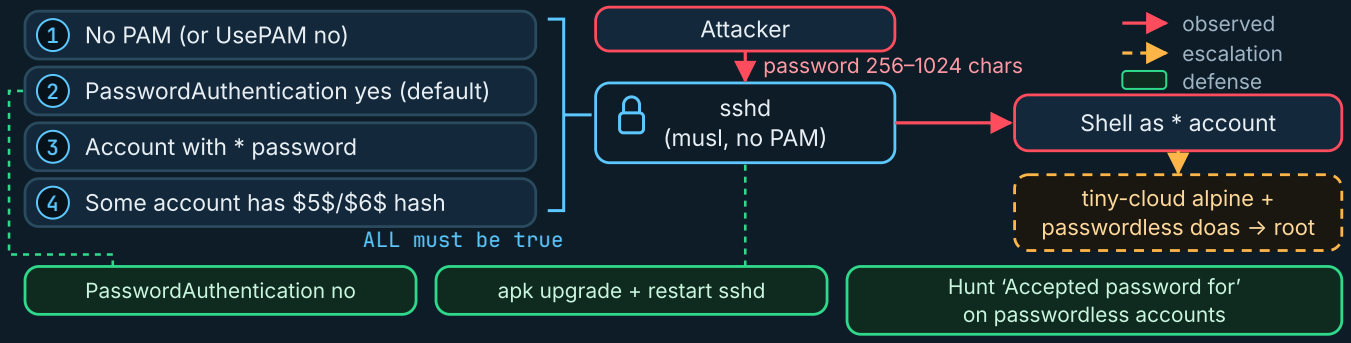


Diagram: MAG212 CYBER, based on [1][22]. KEV added 9 Nov, due 12 Nov; exploiter unknown.

WHO IS EXPOSED · WHAT TO HUNT

- `*` accounts: root, key-only users, directory users without shadow entries
- Tiny-cloud **3.18.11–3.24.3**: `alpine` has `*` **and passwordless doas**; Alpine-based containers inherit [22]
- `Accepted password for` in `/var/log/messages`; doas use, new users, `authorized_keys`
- Can't rule a login out: **treat as compromised**

ALPINE BRANCH → FIXED openssh

edge	10.6_p2-r0	3.24	10.3_p1-r2
3.23	10.2_p1-r1	3.22	10.0_p1-r11
3.21	9.9_p2-r1	3.20	9.7_p1-r6
3.19	9.6_p1-r3	3.18	9.3_p2-r4
3.17	9.1_p1-r7	3.16	9.0_p1-r6

Also 3.21.10, 3.22.8, 3.23.8, 3.24.4. Backported: check the **package revision**, not `sshd -V` [22].

Linux (Alpine) · sshd | root | READ-ONLY | NOT TESTED BY MAG212

SSH-1 · effective setting

```
sshd -T | grep -i passwordauthentication
```

yes: condition met; **no**: mitigated [22][23]

Alpine · apk · OpenRC | root | CHANGES SYSTEM | NOT TESTED BY MAG212

SSH-2 · fix + restart

```
apk upgrade -U -a
rc-service sshd restart
```

Keep a session open; then check the revision.

Alpine · root shell | root | CHANGES SYSTEM | NOT TESTED BY MAG212

SSH-3 · disable password auth

```
mkdir -p /etc/ssh/sshd_config.d
echo 'PasswordAuthentication no' >
/etc/ssh/sshd_config.d/
00-no-passwords.conf
# then Alpine's sed -i.bak edit: copy it
verbatim from the advisory
sshd -t && rc-service sshd restart
```

Interim mitigation if you cannot upgrade [22]. `-t` only checks config and keys [23]: on errors, do not restart. Confirm with SSH-1; check key login works before closing your session.

Order: SSH-2 → else SSH-3 → rebuild images → isolate. **Prevent:** key-only SSH, trusted network, central logs.

Sources: [1] CISA KEV · [2] CVE · [21] OpenSSH notes · [22] Alpine 5 Nov · [23] sshd(8) · [24] 4353fdc

CONFIRMED BY VENDOR · CURSOR, NOTION | FIREWORKS VIA BLEEPINGCOMPUTER | PART 1 OF 2

One vendor key, two downstream breaches

Cursor traces the malicious **Anthropic.claude-code** builds of 29 Oct to a key it gave inference vendor **Fireworks**, which exposed it [26]. Notion data also leaked via Fireworks [34][35].

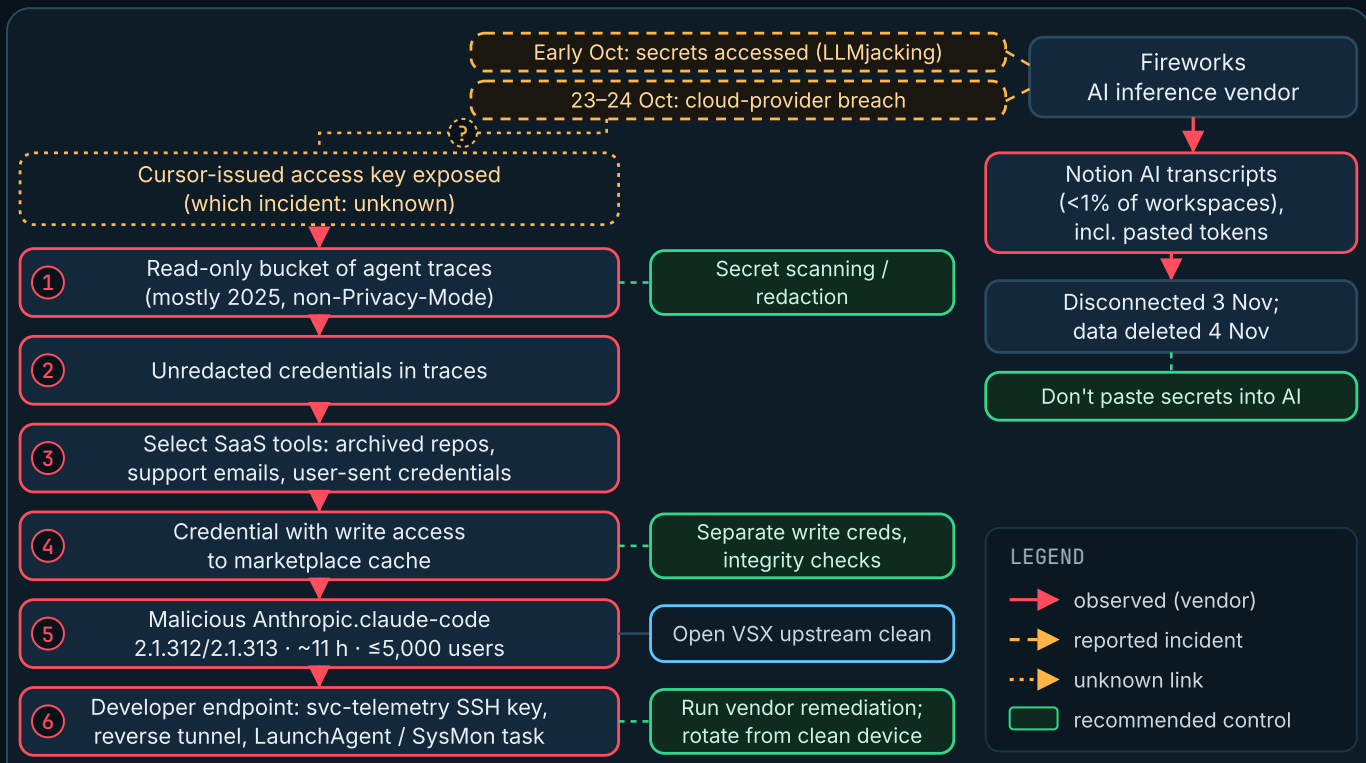


Diagram: MAG212 CYBER, based on [26][27][31][34]. Cursor does not say which Fireworks incident exposed its key; the link is not asserted.

WHAT THE ATTACKER REACHED

- Via unnamed "select SaaS tools": archived non-production repos, support emails, usage metrics and contact details, some conversation summaries, and **credentials users sent to support**
- One credential wrote **directly into the cache serving Cursor's VS Code marketplace**. Open VSX "never had the malware"; not an Anthropic vulnerability [26]

THE FIREWORKS / NOTION LINK

- Notion AI chat transcripts (for Insights) exposed via Fireworks in **<1% of workspaces**, incl. typed API tokens, despite a zero-retention contract [34][35]
- Fireworks also disclosed **early-Oct** env-var secret access (LLMjacking group) and a **23–24 Oct** cloud-provider breach: metadata, billing data, partial model weights and datasets [31]

WHO IS AFFECTED

- **Cursor users** who installed 2.1.312/2.1.313 **from the Cursor marketplace** on Windows or macOS, ~2:27 AM–1:35 PM PT, 29 Oct [27]: at most **5,000** users [26]
- **Notion** workspaces notified by Notion [34]; **Fireworks** customers per its bulletins [31]
- **Credential holders** notified by Cursor; admins got key lists. **<0.01%** of customers had API credentials exposed; **<0.05%** of non-Privacy-Mode users had traces exposed. No notice = not in the traces [26]

Sources: [26] Cursor update 13 Nov · [27] Cursor notice 29/30 Oct · [31] BleepingComputer 10 Nov · [34][35] Notion 9 Nov

PART 2 OF 2 | CLEAN 2.1.314 SHIPPED | UPDATING DOES NOT REMOVE THE BACKDOOR

Hunting the claude-code backdoor

A 66-line `extension.js` loader gathers env-var *names* and the git email, adds an SSH key, tunnels out and persists [27]. Updating to clean **2.1.314** does not remove it [28].

INDICATORS · DEFANGED · FROM CURSOR [27]

Network	`134[.]209[.]82[.]225` · reverse SSH to TCP 22 · HTTP POST to port 8099, path `/beacon`
SSH key	comment `svc-telemetry` in `authorized_keys`
macOS	`~/.config/.smt` · `~/.config/.smtk` · `$TMPDIR/.stk_<10hex>` · `~/Library/LaunchAgents/com.apple.sysmond.plist`
Linux	`/tmp/.stk_<10hex>` · cron `@reboot` running `~/.config/.smt`
Windows	`%USERPROFILE%\.config\smt.cmd` · `%USERPROFILE%\.config\smtk` · `%TEMP%\.stk_<10hex>` · task SysMon · `sysmon.cmd` in Startup
Processes	`ssh -N -R` · `autossh -M 0` · `schtasks /create /tn SysMon`
VSIX hashes	Per-version, per-platform SHA-256 on Cursor's notice: take them from there

False positives: a task named SysMon can collide with Sysinternals Sysmon: check what it executes. `com.apple.sysmond` is a **user** LaunchAgent masquerading as an Apple service.

INVESTIGATE

- **Endpoint:** VSC-1, then Cursor's `grep` (macOS) / PowerShell (Windows) key checks [27]
- **Credentials:** separately, via admin key lists and audit logs

Win/macOS/Linux · code | user

READ-ONLY | NOT TESTED BY MAG212

VSC-1 · list extensions

```
code --list-extensions --show-versions
```

Look for **anthropic.claude-code 2.1.312/2.1.313**. VS Code syntax [30]; `cursor` reportedly accepts it (undocumented) [29]. A match is a lead: confirm with Cursor's VSIX hashes.

CONTAIN & REMEDIATE · IN ORDER

1. Isolate hosts with the `svc-telemetry` key or other IOCs
2. Run `remediate-macos.sh` (as user, **not** root) or `remediate-windows.ps1` (as Administrator), or rebuild [27]
3. Rotate credentials Cursor or Notion named, plus secrets pasted into Notion AI or sent to Cursor support, **from a trusted device** [26][34]
4. Update to 2.1.314 or later
5. Scoping help: security@cursor.com [26]

VERIFY RECOVERY

Old keys fail an authorised test; key and persistence gone; versions match your approved list.

PREVENTION

Developers: keep secrets out of prompts, agent sessions and support tickets; prefer Privacy Mode or zero-retention settings.

Leaders: ask AI vendors which sub-processors see your data and how retention is verified; ask for Cursor's fixes: new inference provider, secret scanning, full rotation, rebuilt store [26].

Sources: [26] Cursor 13 Nov · [27] Cursor 29/30 Oct · [28] ISMG · [29] AiCybr · [30] VS Code docs · [34] Notion

FEATURE 7 REPORTED BY RESEARCHERS bee-js: GHSA-hh7j-5m3j-23pf

wfx: hijacked GitHub accounts steal CI secrets

Since 10 Nov: ~**61,764** repos probed · **1,806+** with credentials stolen · **8,926** with payload [36]

> STATUS **Reported by researchers** (Endor Labs, 12 Nov, upd. 13 Nov) [36]; BleepingComputer's 4,800-account headline not fetched [37]; no GitHub response. bee-js: **secondary aggregation** [38].

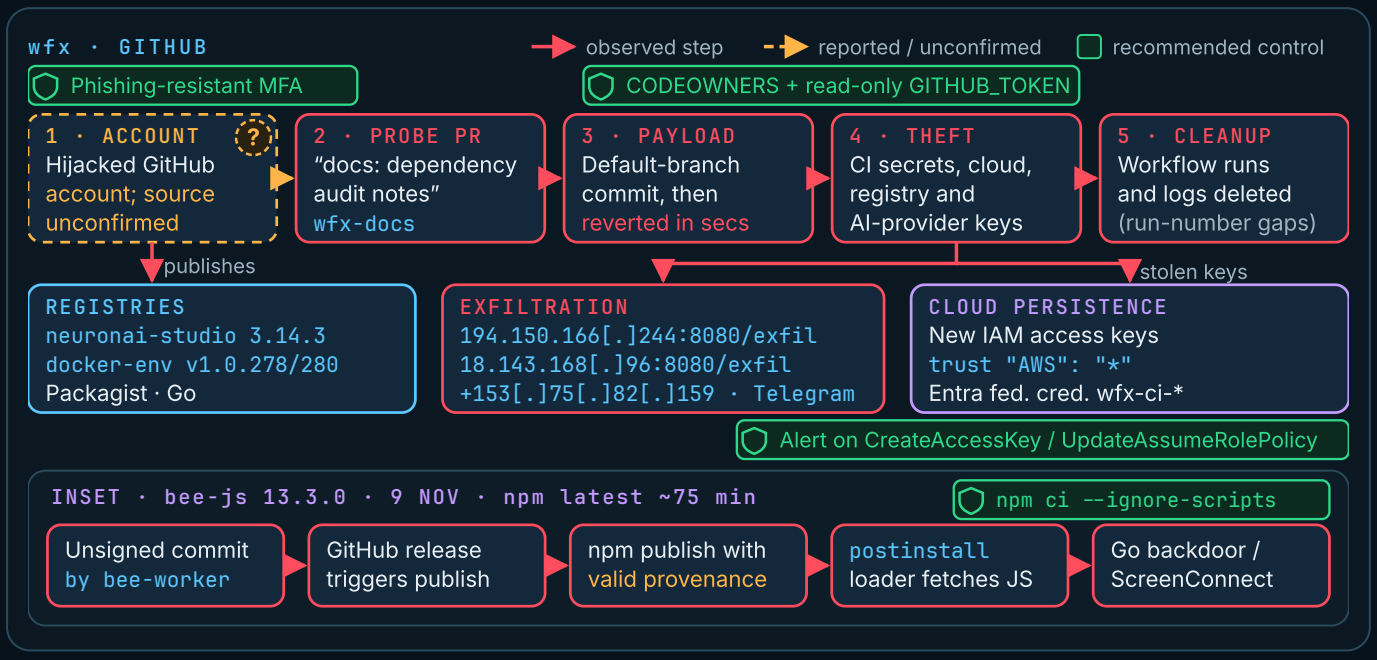


Diagram: MAG212 CYBER, based on [36][38]. One leaked gh OAuth token found; initial access unconfirmed.

WHAT TO LOOK FOR · IOCs (DEFANGED)

EXFIL	194.150.166[.]244:8080/exfil, 18.143.168[.]96:8080/exfil, 153[.]75[.]82[.]159:8080 [36]
STEALER	SHA-256 89695abb392d5cfd4972672961e644bb46baa98aa1ed7173c2a2816c762735cf
BRANCHES	wfx-docs, chore/[a-z0-9]{8}, ci-check-[0-9]{4}; gaps in workflow run numbers
CLOUD	CreateAccessKey, UpdateAssumeRolePolicy, AssumeRoleWithWebIdentity; Entra wfx-ci-*
bee-js	loader ee2f762e9ed3fd89f106e0b80c2e923bf1aed9a280277d3d998a5902c4d9ec0f; DNS frameworkmetrics[.]xyz; solidity-langsupport-runner.service, com.solidity.langsupport.runner; C2 193[.]57[.]9[.]155:4912, 185[.]232[.]84[.]169:8041 [38]

Investigate: PRs "docs: dependency audit notes" since 10 Nov; add-then-revert pairs. **FP:** routine key rotation.

ANY OS · npm NORMAL USER

READ-ONLY NOT TESTED BY MAG212

NPM-1 · bee-js in the full tree

```
npm ls @ethersphere/bee-js --all
```

Any 13.3.0 means the malicious version was installed: treat that machine as compromised. Run per project and CI cache [39].

CONTAIN & REMEDIATE · IN ORDER

1. Revoke sessions, tokens, SSH keys, OAuth grants.
2. Require phishing-resistant MFA.
3. Rotate **every** secret reachable from workflows.
4. Delete attacker IAM keys, "AWS": "*", wfx-ci-*.
5. bee-js: pin 13.2.0 / Desktop 0.56.3, rotate from a clean machine, move funds, rebuild [38].

Verify: no search hits, no unknown IAM/Entra creds, no 13.3.0.

Sources: [36] Endor Labs 12 Nov · [37] BleepingComputer, not fetched · [38] Safeguard.sh 13 Nov · [39] npm-ls docs

FEATURE 8 QUBOLE · RESEARCHERS RAILWAY · VENDOR REPORT ANTIFOX · ONE SOURCE

When the vendor's identity is the attacker

14–26 Oct · correct External ID every time · 100+ secrets in ~7 min, no writes (Sentra) [40]

STATUS Qubole: **reported by researchers** (Wiz, Sentra, Mandiant) via BleepingComputer, CSO [40][41]; AWS: "not compromised… operated as designed". Railway: its report via BleepingComputer [44]. AntiFox: one source [45].

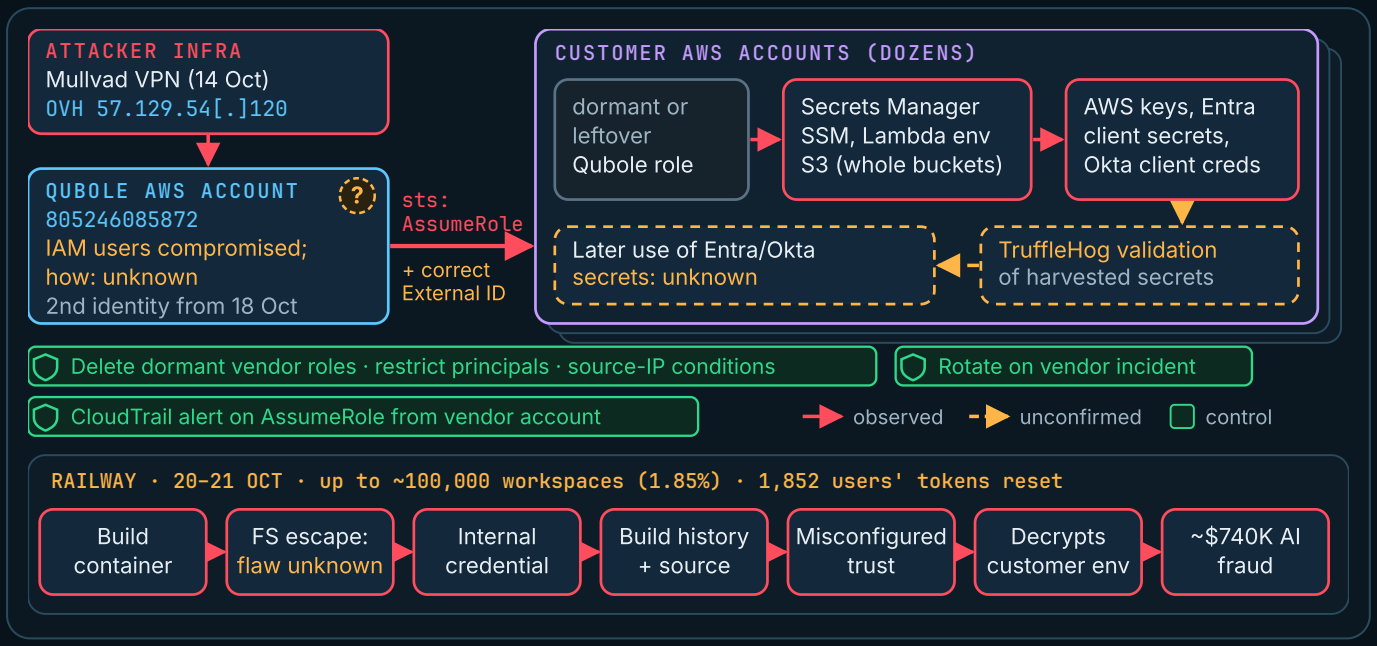


Diagram: MAG212 CYBER, based on [40][41][44]. Railway's 100,000 is a stated maximum, not a confirmed count.

WHAT TO LOOK FOR

QUBOLE	IAM user `AIDA3W7DIFLYOLTK63SFS` · source IP `57.129.54[.]120` · `sso_agent.iso` on attacker infrastructure (TCP 23458; deployment not confirmed)
CLOUDTRAIL	From 1 Oct (named by Wiz): `AssumeRole`, `ListBuckets`, `ListObjects`, `HeadObject`, `GetObject` [40]
ANTIFOX	successful calls hidden inside bursts of `AccessDenied` [45]

Investigate: filter CloudTrail for `AssumeRole` where the caller's account is 805246085872, follow each session; treat every readable secret as exposed. *Syntax unverified: no commands.* **FP:** real Qubole jobs.

CONTAIN & REMEDIATE · IN ORDER

1. Revoke the role's active sessions.
2. Rotate every secret it could read, incl. Entra service-principal and Okta OAuth client secrets.
3. Delete unused vendor integrations.
4. Narrow trust to specific vendor principals; add source-IP or VPC-endpoint conditions.
5. Require IMDSv2; enable GuardDuty.
6. **Railway:** rotate every stored env var; re-link GitHub and AI-provider tokens.

Verify: no roles trust departed vendors; old secrets fail; no odd Entra/Okta sign-ins by rotated clients [40][45].

ANTIFOX · VIA ARCTIC WOLF

Agentic pentest platform (ARTEX fork, on Alibaba Cloud). IIS webshell harvested connection strings, then probed AWS; hundreds of API calls in ~30 min; S3 data copied and deleted. AI agents' role **not** stated [45].

PREVENTION

An External ID stops the confused-deputy problem, **not** a compromised vendor. Treat vendor roles as standing access: review quarterly; delete on contract end.

Sources: [40][44] BleepingComputer 10 Nov · [41] CSO 10 Nov · [42][43] not fetched · [45] BleepingComputer 11 Nov

FEATURE 9 CONFIRMED BY GOVERNMENT · DOJ 26-1351 BINANCE / FACESTEALER · THE RECORD

Operation Endgame hits Gootloader

25,000+ PCs infected since 2018 [47] · **235 servers, 257 domains** disrupted [48] · no arrests

STATUS **Confirmed by government:** DOJ Press Release 26-1351, 12 Nov [47]. Binance and FaceStealer: The Record, 12 Nov; DOJ/FBI releases not fetched [51]. Europol's totals **unverified** [48].

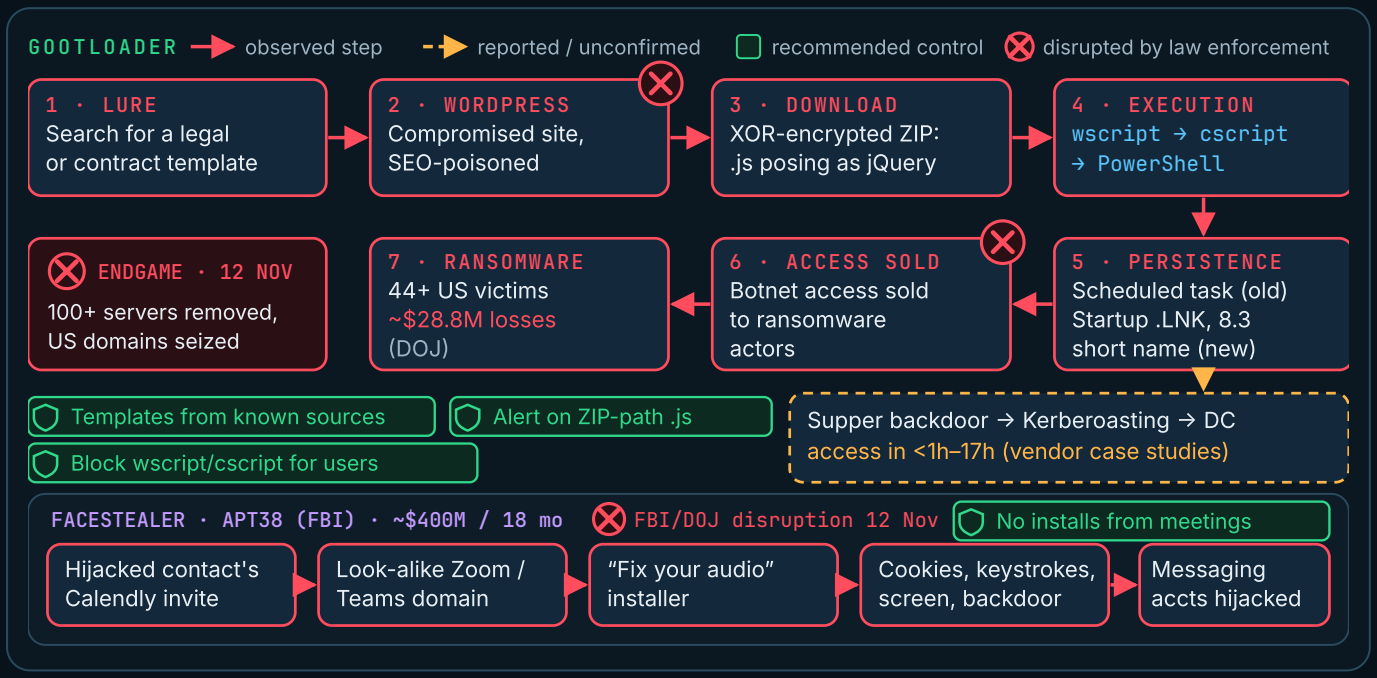


Diagram: MAG212 CYBER, based on [47][49][50][51]. Steps 2–5: vendor research, not DOJ.

WHAT TO LOOK FOR · RED CANARY [50], HUNTRESS [49]

SCRIPTS	`wscript.exe` with an AppData `.js` path (e.g. `AppData\Local\Temp\Temp1_<name>.zip`); `cscript.exe` running a `~1.js` 8.3 name ("an uncommon pattern"); `wscript` → `cscript` → PowerShell
PERSIST	`.dat`/`.log` files renamed to `.js` in AppData\Roaming; scheduled tasks named with 2–3 unrelated words; staging folders mimicking Teams, Zoom, FortiClient, Adobe, UltraVNC
REGISTRY	`HKCU\SOFTWARE\Microsoft\Phone|Personalization|Fax\%USERNAME%`
C2 (2025)	`103.253.42[.]91`, `178.32.224[.]219` (historical, Huntress Nov 2025)

FP: admin `wscript` use, rarely from ZIP temp paths. **FaceStealer:** non-vendor meeting domains.

CONTAIN · IN ORDER

1. Isolate hosts with execution evidence.
2. Reset creds, Kerberoastable accounts first.
3. Rebuild compromised WordPress sites from trusted code.
4. FaceStealer: revoke messaging sessions and tokens; move crypto to new wallets.

Investigate: Shadowserver notices; if persistence is found, scope Kerberoasting and DC access at once. **Verify:** no persistence left; site files match originals.

BINANCE THEFT FUNDS

DOJ got court authorisation to seize or restrain **$1.2B+** of October's ~$6.3B Binance theft (part of $2.7B frozen by platforms); Binance and FBI blame North Korea's TraderTraitor. FaceStealer's role unclear [51].

WHO IS AFFECTED

Lure victims (endpoint fix) and hacked WordPress operators (site fix): the takedown **does not clean hosts**. FaceStealer targets crypto, finance, executives; watch for "fix" installers run after calls.

Sources: [47] DOJ 12 Nov · [48][51] The Record 13, 12 Nov · [49] Huntress 2025 · [50] Red Canary

FEATURE 10 FRANCE · GOVT-CONFIRMED US ADVISORY · REPORTED ICS · SECURITYWEEK

Cold-chain sabotage gets a name

France blames IRGC-linked **SHAHID KAVEH** for the 11–12 Oct attack on **700+** sites [53]

> STATUS France: **confirmed by government** (MFA, 9 Nov) [53]. US joint advisory (CISA, FBI, HHS, USDA, DOT): **reported** by THN, 9 Nov; CISA page not retrieved [52]. ICS: SecurityWeek [55].

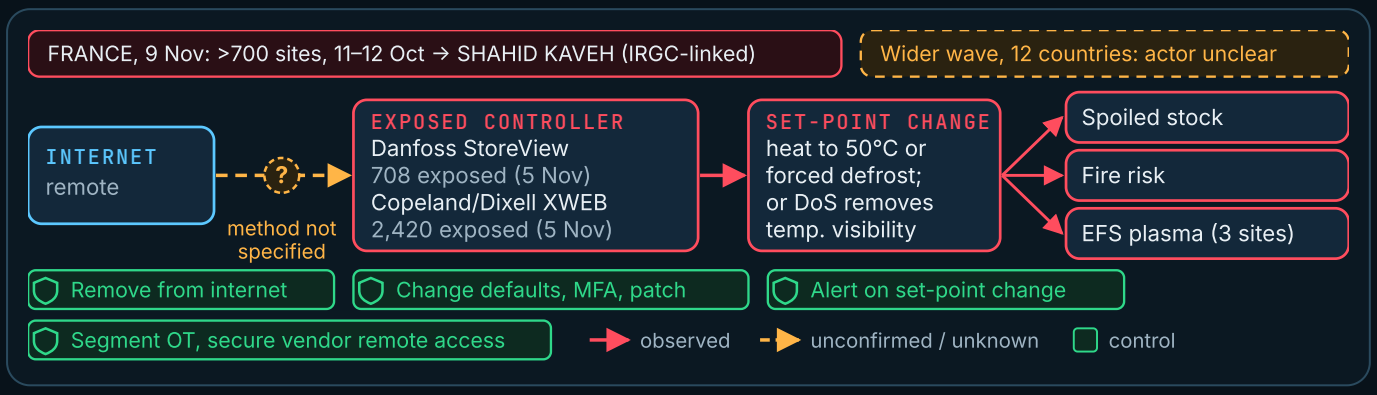
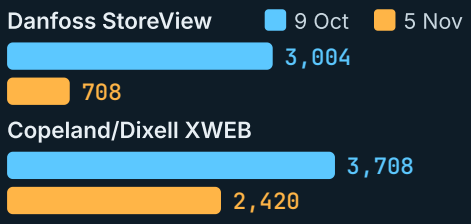


Diagram: MAG212 CYBER, based on [52][53]. No IOCs were published in the sources fetched.

CENSYS EXPOSURE · VIA THN



Internet-exposed instances, **not compromises**; Danfoss mostly in France [52]. Sekoia write-up unfetched [94].

WHAT TO LOOK FOR · INVESTIGATE

- Unexpected set-point or defrost-schedule changes; lost telemetry.
- Web-UI logins from outside your vendor's known addresses (MAG212 inference).
- Inventory controllers, test reachability, pull audit and vendor-session logs, compare set-points with baselines.

France: fires and food losses of "several tens of millions of euros"; Iran's ambassador summoned, EU sanctions to be proposed [53].

CONTAIN & REMEDIATE · ADVISORY, PER THN [52]

1. Remove controllers from internet exposure.
2. Change default passwords; strong auth.
3. Patch.
4. Isolate OT networks.
5. Remove or secure remote access.
6. Retire legacy devices.

Verify: external scan shows controllers unreachable; set-points match baseline; alarms reach on-call staff.

ICS PATCH TUESDAY · 10 NOV · SECURITYWEEK [55]

Siemens · 9 advisories, 10 vulns, 2 with **Node2Shell** impact. High: ROS#, Simcenter Femap, Mendix Studio Pro MCP Server, Simatic SCADA and PCS 7, SIMATIC IOT2050, Simatic WinCC Graphics Designer. Low: FortiGate NGFW in Ruggedcom APE1808. Some unpatched.

Schneider · SEVD-2026-314-01, EcoStruxure Power Build Rapsody (malicious files can lead to code execution).

CERT@VDE · 8 advisories (Beckhoff, MB Connect Line, Helmholz, Weidmueller, Bender, ads-tec), several PHP2Shell.

Phoenix Contact · PHP2Shell, PLCnext. **Hitachi Energy** · 1+ product, PHP2Shell. **Rockwell, ABB** · none.

Johnson Controls · EasyIO Neo IO Manager (priv-esc, code exec); C•CURE 9000 3.20 / victor 8.0 installer may expose admin creds.

Node2Shell (CVE-2026-111497) KEV due **10 Nov** [56]; ICSA-26-316-02 not read [58].

Sources: [52] THN 9 Nov · [53] French MFA 9 Nov · [54][58][94] not fetched · [55][56] SecurityWeek

§5 · DATABASE AND PATCH RELEASES NO EXPLOITATION STATED PG 14 · END OF LIFE

PostgreSQL fixes 52 CVEs; 14.x reaches end of life

"52 security vulnerabilities and over 140 bugs" fixed; **32 of the 52 score CVSS 8.8**, most letting low-privileged authenticated users execute arbitrary code. No in-the-wild exploitation stated [64].

18.7 17.12 16.16 15.20

14.25 · FINAL 19 RC2 · GA 19 Nov

psql · ANY OS ANY ROLE READ-ONLY

NOT TESTED BY MAG212

PG-1 · check server version

```
SELECT version();
```

Run on each primary and standby; managed builds: check the provider's patched build [67].

CVE	CVSS	ISSUE
CVE-2026-6460	lead	Type confusion: object creator runs code as the OS user, mainly via `ALTER … SET DATA TYPE` [65]
CVE-2026-14661	8.1	dblink and subscriptions can append to arbitrary files
CVE-2026-116314 CVE-2026-116330	8.8	`pg_restore`/`pg_dump` code and command execution
CVE-2026-120145	8.8	Logical replication can write subscriber catalogs
CVE-2026-116322	5.3	Pre-authentication spinlock leak [64]

AFTER UPDATING · PER THE 12 NOV ANNOUNCEMENT

- Reindex suspect GIN and pg_trgm GiST indexes
- `REINDEX TABLE` on "missing chunk number" errors
- New full backup if you use incremental backups
- Reindex B-tree on length-less `bpchar` columns
- Check partitioned `NOT NULL NO INHERIT` [66]
- *Correction:* no same-transaction extension rebuild

OTHER PATCH WAVES

FORTINET · 10 NOV

89 advisories, none exploited

- CVE-2026-126170 FMG/FAZ GUI RCE, only if JSON API on (default off)
- CVE-2026-126261 FMG FGFM port, unauth RCE
- CVE-2026-126253 FortiOS OSPF auth bypass
- CVE-2026-126147 FortiMail, unauth RCE
- CVE-2026-126229 dmserver authz bypass [57][60]
- ~17 critical (SecurityWeek) or 19 (Core Sentinel); "Fortinet2Shell" needs FortiPAM [59]

SAP · 10 NOV

38 notes, four at CVSS 10.0

3778530 · CVE-2026-76964 · Kernel ICM
3778556 · CVE-2026-89126 · Web Dispatcher*
3798345 · CVE-2026-89103 · SAP Gateway
3849308 · CVE-2026-120017 · ABAP SAML 2.0 SP

*incl. HANA XSC/XSA. CSO: the first two are Onapsis' **"ICM2Shell"** (WebSocket sequence → crash or RCE) [14]. "PROXYGATE" mapping unverified [63]. Not exploited [62].

ADOBE · MOZILLA · ANDROID · APPLE

Adobe: 110 CVEs, 22 critical. Connect APSB26-191: 24 CVEs, six at 10.0; AEM APSB26-189: four critical RCEs at 9.9. Not exploited [14].

Firefox CVE-2026-124907**:** WebGL UAF + sandbox escape; Firefox 160, Thunderbird 160/153.7. **Android:** 216 fixes, 23 critical [14]. **Apple:** no zero-day.

OTHER KEV ADDITIONS

GPUStack CVE-2026-102895 · 9.8 · spoofable loopback treated as admin [1][86] · fix 2.2.0

FreeSWITCH CVE-2026-116779 · 9.8 · SIP "To" `api+…` reaches `switch_api_execute()` [87] · fix 1.11.3

IBM Aspera Faspex CVE-2026-123218 · 9.8 · 5.0.0–5.0.19; CNA PR:N vs "authorized user" [88] · fix per IBM

Cisco BroadWorks CVE-2026-20320 · 7.5 · XXE [90]; "Operation Snowball" [61] · fix Aug 2026

Openwave Webtop CVE-2026-111793 · 4.3 · Media Transcoder [91] · fix 1.1.22.0

UnrealIRCd CVE-2026-114713 · 8.6 · IRCv3 `label` injection on linked networks [89] · fix 6.2.7.1

§5 BRIEFS · BREACHES, EDUCATION, AVIATION, POLICY

Breaches, schools and a non-cyber ground stop

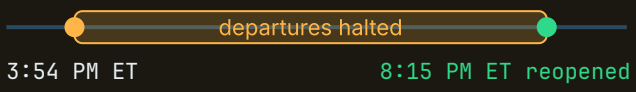
NOT A CYBERATTACK

FRI 13 NOV · AVIATION

FAA ground stop: overloaded network gear, not hackers

Departures halted nationwide "following communication issues impacting multiple Air Route Traffic Control Centers" [77][78]; Duffy said "all" [79].

Stated cause: switches and routers overloaded with data after new technology was added to older components: intermittent communication and radar gaps, no total loss. **DHS Secretary Markwayne Mullin said there was no cyberattack** [78].



4,700+ cancellations and ~10,000 delays Fri; ~700 cancellations already Sat [78]

Longest stop in 25 years (Al Jazeera, which says both "five hours" and "more than four hours"). No root-cause report, facility or vendor named.

Lesson for network engineers: a capacity and change-management failure; load-test legacy networks before connecting new systems.

BREACHES AND RANSOMWARE · NOTION: FEATURE 6 · RAILWAY: FEATURE 8

Maersk · Confirmed 11 Nov: a legacy system of acquired LF Logistics was breached and data stolen; no operational, API or EDI impact. Claim only: WhiteArmor says ~100 GB, $5M BTC in 30 days, ~30,000 driver records with plaintext passwords [69]

TSMC · Told the SEC (~12 Nov) employee data held by an unnamed **cloud service provider** was exposed; own systems not compromised. Claim only: 6.9 GB sale for 3 BTC [70]

City of Osaka · 1M+ addresses exposed via Arara, used by vendor TKC; Arara's 2 Nov breach hit 77M addresses at ~400 customers and fed bank phishing [72]

Apify · Access 9–10 Nov via "a compromised credential", cut off 11 Nov; secrets rotated, some OAuth (incl. GitHub) revoked, tokens now hash-only [68]. Reconnect GitHub, set storage to Restricted; treat pre-11 Nov tokens as exposed (MAG212 inference).

ActiveCloud · Belarus provider's ransomware outage of E-Cloud and SmartMail; restored by 13 Nov. Russia's ESTT and Beget (wiper) also hit; no public link [71]

Baker Tilly · Amplifon · Third-party platform exposed names, addresses, SSNs [74]. Amplifon: SSNs and medical data stolen Jan–Feb 2026; Texas counts 85,804; 1.33M unconfirmed [75]

POLICY AND ATTRIBUTION

UK NCSC · Launched **Cyber Adversary Simulation (CyAS)** on 11 Nov: an MVP for critical organisations and regulators, no mandatory requirements [83]

White House · AI task force urged easing cyber liability so AI firms report critical incidents (Bloomberg, not fetched) [84]

FBI · ARTEX · Reported warning on the "ARTEX" autonomous pentest framework (~13 Nov, unverified); AntiFox is a fork [93]

Qilin · Admin "Haise" allegedly unmasked; firms named Aleksey Mikhailovich Yakovtsev. Low confidence [73] [76]

Context · SonicWall CVE-2026-19868 KEV due 20 Nov [92]; Node2Shell KEV deadline fell 10 Nov [56].

EDUCATION

UT Arlington · Confirmed 13 Nov data stolen in October; MachForms portal still offline; Qilin claims it (claim only) [73]

Vanderbilt · Restoration could take "multiple weeks"; BYOD gang claims it [73]

Richmond PS · 21 Oct data "may now be on the dark web" (not confirmed); credit monitoring offered [80]

New Plymouth SD · Network and Google accounts shut after a 10 Nov "cyber threat"; classes cancelled 11–12 Nov [81]

Easthampton · No data theft found; $10,000 deductible vs an estimated >$100k uninsured cost [82]

Lesson: plan offline continuity; confirm insurance terms now.

§6 · KEV 2026.11.13 [12 KEV ADDITIONS] [6 DEADLINES PASSED] [2 DUE MON 16 NOV]

KEV and patch board



ADD→DUE	CVE	PRODUCT	WEAKNESS	CVSS	FIX
9 → 12	CVE-2026-102895	**GPUStack**	Improper authentication	9.8	2.2.0 [86]
9 → 12	CVE-2026-116779	**SignalWire FreeSWITCH**	Code injection	9.8	1.11.3 [87]
9 → 12	CVE-2026-123158	**OpenSSH (“SSHole”)**	Password-auth bypass (musl, no PAM)	8.1	10.6p2 / distro [21][22]
9 → 12	CVE-2026-123218	**IBM Aspera Faspex**	Incorrect authorization	9.8*	Per IBM [88] (5.0.0–5.0.19)
10 → 24	CVE-2026-125350	**Google Chromium**	Use-after-free (XML)	8.8	Chrome 157.0.8103.50/.51 [20]
10 → 13	CVE-2026-116606	**Barracuda ESG**	Auth bypass (alt. path)	9.3†	BNSF-40425 / 40430 [11]
10 → 13	CVE-2026-111560	**Barracuda ESG/ADC/BMA/ WCC/WAF/WSG**	OS command injection	8.6†	Per-product patch [11]
10 → 24	CVE-2026-20320	**Cisco BroadWorks**	XXE	7.5	Fixed Aug 2026 [90]
10 → 24	CVE-2026-111793	**Openwave Webtop Media Transcoder**	Resource transfer between spheres	4.3	1.1.22.0 [91]
10 → 24	CVE-2026-124194	**Microsoft Outlook**	Missing unsafe-action warning (NTLMv2 leak)	6.5	Nov Office update [2]
13 → 16	CVE-2026-123039	**Check Point (Gaia)**	Incorrect permissions (DynamicCLI)	7.8	JHF takes per sk1000362 [3]
13 → 16	CVE-2026-114713	**UnrealIRCd**	Delimiter injection	8.6	6.2.7.1 [89]

Nov dates; red = passed, amber = due within 2 days. All cite BOD 26-04, ransomware use “Unknown” [1]; 9 Nov batch confirmed [25] [85]. CVSS: CNA [2], †v4. *CNA record inconsistent (PR:N vs “authorized user”). 3-day deadlines appear to follow BOD 26-04 risk tiers (unconfirmed).

MAJOR PATCH RELEASES THIS WEEK

Microsoft · 10 Nov · 1,093–1,094 CVEs, 63 critical
Office LTSC 2021 16.0.14334.21048; LTSC 2024 16.0.17932.21140; M365 Apps by channel [2][17] · ***exploited***

Google Chrome · 9 Nov · 9 security fixes (8 CVEs listed)
157.0.8103.50/.51 Win/Mac; .50 Linux [20] · ***exploited*** *(KEV)*

Check Point · sk 8–12 Nov · CVE-2026-123039
R82.20 T14+, R82.10 T52+, R82 T132+, R81.20 T174+ [3] · ***exploited***

Barracuda · 2–9 Nov · CVE-2026-116606/111560
BNSF-40425/40430, BNADC-16586, BNMA-32468, BNWF-60060, BNYF-24789 [11] · ***exploited***

N-able N-central · 10 Nov · 7 CVEs (HF2)
2026.4 HF2, build 2026.4.1.26, plus Agent/Probe upgrades; Legacy API off or unexposed [10] · *exploitation disputed*

OpenSSH / Alpine · 5 Nov · CVE-2026-123158
10.6p2; Alpine revisions per Feature 5 [21][22] · ***exploited***

PostgreSQL · 12 Nov · 52 CVEs
18.7, 17.12, 16.16, 15.20, 14.25 (14 is EOL) [64] · *expl. not stated*

Fortinet · 10 Nov · 89 advisories, ~17–19 critical
FortiOS 8.0.2/7.6.8/7.4.13/7.2.14; FMG/FAZ 7.6.8/7.4.12; FortiMail 7.6.7/7.4.9 (7.2 must migrate; 8.0.2 clears criticals, one high awaits 8.0.3). Verify on FortiGuard [57][60] · *not exploited*

SAP · 10 Nov · 38 notes, 4 × CVSS 10.0
3778530, 3778556, 3798345, 3849308 [62] · *not exploited*

Adobe · 10 Nov · 110 CVEs
Connect APSB26-191; AEM APSB26-189 [14] · *not exploited*

Mozilla · Nov · CVE-2026-124907
Firefox 160; Thunderbird 160 / 153.7 [14] · *expl. not stated*

Android · Nov · 216 fixes, 23 critical
November bulletin [14] · *expl. not stated*

Siemens / Schneider / VDE · 10 Nov · Siemens 9; SEVD-2026-314-01; VDE 8
Some Siemens products unpatched; use mitigations [55] · *Node2Shell attempts seen, not vs Siemens*

Cursor / Anthropic ext. · Oct 29–Nov 13 · Malicious 2.1.312/2.1.313
Clean 2.1.314 (updating does not remove an installed backdoor) [28] · ***exploited*** *(supply chain)*

bee-js / Swarm Desktop · 9 Nov · Malicious 13.3.0 / 0.56.2
13.2.0 pinned / Desktop 0.56.3 [38] · ***exploited*** *(supply chain)*

§7 DEFENDER'S ACTION DESK · CP-/SSH-/NPM- = FEATURE COMMAND PANELS

Nineteen actions, three deadlines

Today

includes KEV deadlines passed or due Monday

01 Run sk1000362 greps (CP-1 to CP-4) on every Check Point gateway, management, MDS and log server; copy `dynamicCli.log` off-box, then install the fixed JHF take. If you cannot patch, disable `dynamic_server` per the sk. KEV due **Mon 16 Nov**. [1][3] NETWORK

02 Confirm Barracuda patches on ESG, ADC, WAF, WSG, BMA and WCC, and that admin UIs are not internet-reachable. KEV due date has passed. [11] NETWORK

03 N-central: confirm the Legacy API is disabled or not internet-exposed, apply HF2, upgrade Agents and Probes, block and hunt `157.20.241[.]16` / `139.99.69[.]109` / `79.76.51[.]56`; review activity since 11 Nov. [10] ENDPOINT / MSP

04 GitHub orgs: search for "docs: dependency audit notes" PRs and `wfx-docs` / `chore/*` / `ci-check-*` branches since 10 Nov. Check workflow run-number gaps. [36] CLOUD / DEVOPS

05 Alpine and musl hosts: run SSH-1. Upgrade and restart `sshd` (SSH-2), or apply SSH-3. Hunt "Accepted password for" on passwordless accounts. [22] ENDPOINT / LINUX

06 Force Chrome to 157.0.8103.50 or later and restart. Update Edge and Opera. [1][20] ENDPOINT

Within 48 hours

next in line

07 Deploy the November Office update by channel for Outlook CVE-2026-124194, and block outbound SMB to the internet. KEV due 24 Nov. [14][17] ENDPOINT / NETWORK

08 CloudTrail from 1 Oct: `AssumeRole` from account 805246085872, IAM user AIDA3W7DIFLYOLTK63SFS, IP `57.129.54[.]120`. Delete dormant vendor roles; rotate secrets they could read. [40] CLOUD

09 CloudTrail `CreateAccessKey` / `UpdateAssumeRolePolicy` / `AssumeRoleWithWebIdentity`, and Entra `wfx-ci-*` federated credentials. Remove any found; rotate workflow-reachable secrets. [36] CLOUD / IDENTITY

10 Cursor, Notion, Apify, Railway notices: rotate the named keys from a clean device. Check dev machines for the `svc-telemetry` SSH key; run Cursor's remediation scripts. [26][27][34][44][68] IDENTITY / ENDPOINT

11 Run `npm ls @ethersphere/bee-js --all` (NPM-1) in projects and CI caches; pin 13.2.0. [38][39] CLOUD / DEVOPS

12 Fortinet: upgrade FortiManager, FortiAnalyzer, FortiOS and FortiMail. Confirm FGFM, admin interfaces and the JSON API are not internet-exposed. [57][59] NETWORK

This week

patch waves, hunting and hardening

13 PostgreSQL: update to 18.7, 17.12, 16.16, 15.20 or 14.25. Complete the post-update REINDEX and backup tasks; plan the PG14 exit. [64][66] ENDPOINT / DBA

14 Apply SAP's four CVSS 10.0 notes (ICM2Shell first) and Adobe Connect/AEM. [14][62] ENDPOINT / APPS

15 OT: find internet-exposed refrigeration/monitoring controllers, change defaults, segment. Review Siemens, Schneider, VDE advisories; inventory Node.js, Brotli, PHP in HMIs. [52][55] NETWORK / OT

16 SOC: hunt Gootloader (`wscript` → `cscript` → PowerShell, ZIP-path `.js`, Startup `.LNK` with 8.3 names); watch for Shadowserver notifications. [48][50] ENDPOINT / SOC

17 Harden CI: CODEOWNERS on workflows, read-only `GITHUB_TOKEN` by default, `npm ci --ignore-scripts`, protected release branches, phishing-resistant MFA for maintainers. [36][38] CLOUD / IDENTITY

18 Review vendor AI sub-processors and data retention (the Fireworks lesson), list every third-party cross-account role, brief staff on fake-meeting scams. [34][40][51] LEADERSHIP

19 Schools: confirm offline-continuity plans, insurance terms, MFA coverage. [81][82] LEADERSHIP / SCHOOL IT

§8 AWARENESS FOR EMPLOYEES AND LEADERS PRINT · PIN · DISCUSS AT MONDAY STAND-UP

Four tricks this week, and what to do instead

1 The attachment that “just opens”

Opening a booby-trapped message or Office file made Outlook quietly contact the attacker's server and hand over a scrambled form of your login (an NTLM hash) [14]. Previewing is not enough; opening is. [15]

DO Be wary of unexpected attached emails (`.msg`) or documents, even from people you know. Check with the sender by phone or chat first. Let IT update promptly.

2 The meeting that asks you to install a “fix”

“FaceStealer” sent invites from hijacked contacts to fake Zoom or Teams pages with deepfaked video, then claimed your audio was broken. The “fix” stole passwords, cookies and keystrokes. The FBI links it to North Korea's APT38 and ~$400 million in thefts. [51]

DO Never install anything during a call. If audio fails, rejoin from the app you normally use. Confirm unexpected invites via a known contact route.

3 The secret you pasted somewhere “safe”

After a key leaked from Cursor's AI vendor, the attacker found passwords and API keys people had typed into AI sessions and **sent to support** [26]. Notion AI input, API tokens included, was exposed for some workspaces via the same vendor. [34]

DO Never paste passwords, API keys or customer data into chatbots, AI assistants or support tickets. If you have, tell IT so it can be changed.

4 The document template from a search result

Gootloader hid behind search results offering legal-style documents and contract templates on hacked sites. The download gave criminals a foothold sold to ransomware gangs; 44 US victims lost about $28.8 million. [47][49]

DO Use your firm's library or known publishers. A ZIP containing a script (`.js`)? Don't open it; report it.

FOR LEADERS · THREE QUESTIONS FOR MONDAY

1 ***Which vendors can reach our cloud, and which ones have we stopped using?***
Qubole's leftover access roles let an attacker into dozens of companies [40]

2 ***Which AI vendors process our data, which providers do they pass it to, and how do we know they delete it?***
Notion found data retained despite a zero-retention promise [34]

3 ***If our remote-management or firewall vendor issued an emergency notice on a Saturday, who would act?***
This week, Check Point, Barracuda and N-able all did [3][10][11]

IF SOMETHING ALREADY HAPPENED

Tell IT immediately, say what you opened and when, and don't delete the email or invite.

Reporting fast is never the wrong call.

FREE SUBSCRIPTION

Get MAG212 CYBER free

Share this lesson with your team.

SUBSCRIBE FREE →

cyber.mag212.com/subscribe-free/

Source register §9 · 94 SOURCES · 1 OF 2

Dates are publication or last update as shown by the source. “Not fetched” means the URL was identified but its content was not read directly; those sources only support claims flagged accordingly. Titles are links.

1 **CISA (GitHub mirror)** · Known Exploited Vulnerabilities catalog JSON, catalogVersion 2026.11.13 · 13 Nov 2026, 20:24 UTC
2 **CVE Program** · cvelistV5 CVE JSON 5 records (CVE-2026-123039, -124194, -125350, -123158, -6460 and others) · Various, Nov 2026
3 **Check Point** · sk1000362: Local privilege escalation to root in the DynamicCLI process via local world-writable control socket · Created 8 Nov, modified 12 Nov 2026
4 **Check Point** · sk98028: Jumbo Hotfix Accumulator FAQ · Undated
5 **Check Point Research** · PHP2Shell exploitation on Check Point gateway (**unreachable**) · Not verified
6 **WindowsForum** · CISA KEV alert: patch UnrealIRCd CVE-2026-114713 and Check Point CVE-2026-123039 · 13 Nov 2026
7 **CTO at NCSC (Substack)** · Summary, week ending November · Nov 2026
8 **The Record** · PHP2Shell: successful exploitation reports emerge · 29 Oct 2026
9 **Cloud Security Alliance Labs** · CSA research note: Able2Shell N-central zero-days · 10 Nov 2026
10 **Huntress** · N-able disables cloud services following disclosure of Able2Shell exploit chains · 9 Nov, updated through 13 Nov 2026
11 **Barracuda Trust Center** · Pre-authentication authorization bypass and command injection · 2 Nov; updated 5 and 9 Nov 2026
12 **Mandiant** · MNDT-2026-0041 (CVE-2026-111560) · Nov 2026
13 **Mandiant** · MNDT-2026-0042 (CVE-2026-116606) · Nov 2026
14 **CSO Online** · November 2026 Patch Tuesday: 63 critical Microsoft fixes plus an Outlook zero-day that allows theft of hashed credentials · 10 Nov 2026
15 **eSecurityPlanet** · Microsoft November 2026 Patch Tuesday: Outlook zero-day · 11 Nov 2026
16 **Microsoft MSRC** · CVE-2026-124194 Security Update Guide entry (**JavaScript-only; not readable**) · 10 Nov 2026
17 **Microsoft Learn** · Update history for Microsoft 365 Apps (by date) · Entries dated 10 Nov 2026
18 **SecurityWeek** · Exploited Outlook zero-day among 1,094 flaws patched by Microsoft (headline only; page not readable) · Nov 2026
19 **IT-Connect** · Patch Tuesday November 2026: Microsoft fixes 1,093 vulnerabilities (not fetched) · Nov 2026
20 **Google Chrome Releases** · Stable Channel Update for Desktop · 9 Nov 2026
21 **OpenSSH** · Release notes (OpenSSH 10.6p2) · 5 Nov 2026
22 **Alpine Linux** · OpenSSH password authentication bypass · 5 Nov 2026
23 **OpenBSD** · sshd(8) manual page · Current
24 **OpenSSH portable (GitHub)** · Commit 4353fdc (SSHole workaround) · Nov 2026
25 **eSecurityPlanet** · CISA KEV adds GPUStack, FreeSWITCH, OpenSSH, IBM flaws · 10 Nov 2026
26 **Cursor** · Security incident update · 13 Nov 2026
27 **Cursor** · Claude Code extension security notice · 29 Oct, updated 30 Oct 2026
28 **GovInfoSecurity (ISMG)** · Cursor confirms Anthropic Claude Code extension compromised · 30 Oct 2026
29 **AiCybr** · Cursor Claude Code extension 2.1.313 marketplace compromise: response · 30 Oct 2026
30 **Visual Studio Code docs** · Command line interface · Current
31 **BleepingComputer** · Fireworks AI discloses new breach after cloud provider hack · 10 Nov 2026
32 **Fireworks AI** · October 2026 security incident (not fetched) · Oct–Nov 2026
33 **Fireworks AI** · October 2026 security incident update (not fetched) · Nov 2026
34 **Notion** · Security incident involving a third-party AI vendor (help centre) · Early Nov 2026 (page undated)
35 **Notion** · Security advisory: third-party AI vendor incident · 9 Nov 2026
36 **Endor Labs** · GitHub Actions supply chain attack targeting CI secrets at scale · 12 Nov, updated 13 Nov 2026
37 **BleepingComputer** · Hackers compromise 4,800 GitHub accounts to steal cloud credentials (not fetched) · Nov 2026
38 **Safeguard.sh** · @ethersphere/bee-js and Swarm Desktop compromise: npm loaders without install scripts · 13 Nov 2026
39 **npm Docs** · npm-ls (CLI v12) · Current
40 **BleepingComputer** · Hackers exploit trusted AWS access to breach multiple cloud environments · 10 Nov 2026 (AWS statement added 11 Nov)
41 **CSO Online** · Qubole supply chain attack exposed AWS, Entra ID and Okta credentials · 10 Nov 2026
42 **Wiz** · Qubole cross-account access abused in the wild (not fetched) · Nov 2026
43 **Sentra** · Inside the Qubole supply chain attack (not fetched) · Nov 2026
44 **BleepingComputer** · Railway breach leads to $740,000 in fraudulent AI charges · 10 Nov 2026
45 **BleepingComputer** · Hackers use AntiFox AI agents in AWS credential theft attacks · 11 Nov 2026
46 **Microsoft Learn** · Block authentication flows with Conditional Access policy · Current
47 **US Department of Justice** · Gootloader malware disrupted in international cyber operation (Press Release 26-1351) · 12 Nov 2026
48 **The Record** · Gootloader: DOJ details takedown · 13 Nov 2026
49 **Huntress** · Gootloader threat detection: WOFF2 obfuscation (background) · Nov 2025
50 **Red Canary** · Threat Detection Report: Gootloader (background) · Undated
51 **The Record** · Stolen Binance crypto recovered; DOJ disrupts FaceStealer · 12 Nov 2026
52 **The Hacker News** · US agencies warn on refrigeration and cold-chain system attacks · 9 Nov 2026
53 **French Ministry for Europe and Foreign Affairs** · Déclaration d'attribution à l'Iran de cyberattaques visant la France · 9 Nov 2026
54 **CERT-FR** · CERTFR-2026-CTI-009 (not fetched) · Not verified
55 **SecurityWeek** · ICS Patch Tuesday: Siemens flags high-severity flaws, Node2Shell exposure · 11 Nov 2026
56 **SecurityWeek** · CISA warns of Node2Shell exploitation as honeypots log attack attempts (background) · 28 Oct 2026
57 **Core Sentinel** · Cybersecurity news roundup, mid-November 2026 (Australia) · 11 Nov 2026
58 **CISA** · ICSA-26-316-02 Siemens Desigo, Gridscale (not fetched) · ~12 Nov 2026 (inferred)

§9 SOURCE REGISTER · 2 OF 2 (CONTINUED)

59 **SecurityWeek** · Fortinet patches nearly 100 vulnerabilities · 11 Nov 2026

60 **Fortinet FortiGuard PSIRT** · FG-IR-26-219, FG-IR-26-275, FG-IR-26-267, FG-IR-26-199, FG-IR-26-244 · 10 Nov 2026 · 219 · 275 · 267 · 199 · 244

61 **The Hacker News** · Cisco BroadWorks and Openwave flaws added to KEV · 11 Nov 2026

62 **Pathlock** · SAP Security Patch Day November 2026 · 10 Nov 2026

63 **BleepingComputer** · SAP patches four maximum-severity security vulnerabilities (not fetched) · Nov 2026

64 **PostgreSQL Global Development Group** · PostgreSQL 18.7, 17.12, 16.16, 15.20, 14.25 and 19 RC 2 released · 12 Nov 2026

65 **PostgreSQL** · CVE-2026-6460 · 12 Nov 2026

66 **PostgreSQL** · 20261112 update release announcement (mailing-list attachment) · 12 Nov 2026

67 **PostgreSQL docs** · System Information Functions · Current

68 **Apify** · Status page incident sxd1dj5j6749 · 11–13 Nov 2026

69 **BleepingComputer** · Maersk confirms data breach as WhiteArmor ransomware demands $5 million · 11 Nov 2026

70 **The Record** · TSMC confirms employee data breach via cloud provider · 13 Nov 2026

71 **The Record** · Belarus cloud provider ActiveCloud hit by ransomware · 13 Nov 2026

72 **The Record** · City of Osaka email data breach · 13 Nov 2026

73 **The Record** · University of Texas at Arlington warns of data breach · 13 Nov 2026

74 **ClassAction.org** · Baker Tilly Advisory Group data breach · Nov 2026

75 **The Record** · Amplifon hearing aid company data breach · ~9 Nov 2026

76 **SOCRadar** · Qilin ransomware admin "Haise" unmasked? · 6 Nov, updated 11 Nov 2026

77 **Federal Aviation Administration** · FAA statement on nationwide ground stop · 13 Nov 2026

78 **Al Jazeera** · FAA ground stop lifted: why were US flights grounded and what's next · 14 Nov 2026

79 **AeroTime** · FAA nationwide ground stop over ATC communications · 13 Nov 2026

80 **WTVR** · RPS cyberattack: data may be on dark web · 11 Nov 2026 (updated 13 Nov)

81 **Idaho Press** · New Plymouth School District shuts down network after threat · 11 Nov 2026

82 **Daily Hampshire Gazette** · No data stolen in Easthampton schools cybersecurity incident, superintendent says · 10 Nov 2026

83 **UK NCSC** · NCSC scheme to help critical organisations test their cyber defences · 11 Nov 2026

84 **Bloomberg** · White House urges easing liability to encourage AI disclosure (not fetched; via [7]) · 14 Nov 2026

85 **DailyCISO** · CISA KEV additions Nov 6 to Nov 9, 2026 · Nov 2026

86 **GPUStack (GitHub)** · GHSA-gj9m-f8ph-pmhr · Nov 2026

87 **SignalWire FreeSWITCH (GitHub)** · GHSA-mg63-h38w-8p9p · Nov 2026

88 **IBM** · Security bulletin, Aspera Faspex (node 7295921) · Nov 2026

89 **UnrealIRCd forums** · Security advisory, CVE-2026-114713 (t=9487) · ~8 Nov 2026

90 **Cisco** · cisco-sa-bworks-xxe-uwUd7CEt · Aug 2026

91 **Openwave / JPCERT JVN** · CAN-2026-2032674; JVNVU93403064 · 2026 · CAN · JVN

92 **SonicWall PSIRT** · SNWLID-2026-0014 (background) · Updated 9 Nov 2026

93 **FBI IC3** · Cybersecurity advisory on ARTEX (date unverified) · ~13 Nov 2026 (inferred)

94 **Sekoia** · The cold chain on fire: unpatched Danfoss controllers exploited (not fetched) · Not verified

HOW WE VERIFIED THIS ISSUE · §10 SUMMARY

- **Checked directly:** the CISA KEV feed (2026.11.13) and cvelistV5 records; Check Point, Barracuda/Mandiant, Chrome, OpenSSH/Alpine and PostgreSQL advisories; Cursor, Notion, Apify and Endor Labs disclosures; DOJ, French MFA, UK NCSC and FAA statements [1][2][3][11][20][22][26][34][47][53][64][68][77][83].
- **Command panels** rest on official documentation only: VS Code CLI, npm-ls, Microsoft Learn and PostgreSQL docs [17][30][39][46][67].
- **Unreachable:** NVD (so CNA CVSS scores are used), MSRC pages, Check Point Research, cisa.gov advisory pages, Europol and several BleepingComputer and SecurityWeek pages [5][16][18][58][63].
- **Identified but not fetched:** Fireworks bulletins, Wiz and Sentra Qubole blogs, CERT-FR CTI-009, Sekoia, Bloomberg, IT-Connect and the IC3 ARTEX PDF; claims resting on them are flagged [19][32][33][42][43][54][84] [93][94].
- **Conflicts resolved by attribution:** Patch Tuesday count (1,094 vs 1,093), Fortinet criticals (17 vs 19), FAA scope ("multiple" vs "all") and duration, Gootloader totals; Check Point scope follows sk1000362; N-central exploitation is printed as **disputed**.
- **Still unverified (flagged or excluded):** the PHP2Shell → DynamicCLI chain, Huntback mining counts, the SSHole exploiter, the Outlook researcher credit, the ARTEX advisory date and the Qilin leader identification (low confidence).
- **Corrected vs the earlier draft:** research cutoff 10:05 AM PST; N-central now disputed; unverified PGDG RPM instruction and the 14 Nov Microsoft 365 outage item removed; PostgreSQL panel switched to doc-verified `SELECT version();`.

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

Weekly · 14 November 2026
Understand the threat. Build the defense.