MAG212CYBER

WORLD REPORT
WEEKEND EDITION · ISSUE 04



COVER ART · MAG212 CYBER

ANALYST EDITION · NOV 1–7, 2026

TRUST WAS THE ATTACK SURFACE

INSIDE

- Ivanti chain beats its checker
- SonicWall SAML/MFA bypass (KEV)
- cPGuard update hijack
- Trojanized Cursor extension
- PaaS secrets & Chainalysis
- APT29 mobile exploit kits
- Barracuda ESG pre-auth root
- Sigma rules + hunt pack

Forty threat briefings from the MAG212 analyst desk: hijacked updates, poisoned extensions, exploited edge systems, and what to fix first.

NOV 7, 2026 | MAG212 CYBER | EL MOSTAFA OUCHEN

CYBER.MAG212.COM PUBLISHED BY MAG212 CYBER

THE WEEK IN ONE PAGE

Attackers didn't break in. They were delivered.

This week the most damaging intrusions arrived through channels defenders are trained to trust: a vendor's auto-update, a marketplace extension, a monitoring script, an identity flow, a PaaS secret store. Patching closed some doors; it did not undo what those channels already carried.

~2,950
Linux servers ran cPGuard's fake root update on Nov 2[1]

3
CISA KEV additions Oct 31–Nov 7: WordPress, Apple, SonicWall[2]

1,379
secrets in public Claude Code approval files (Apiiro)[3]

1.3M+
Android TV boxes with factory XCPE backdoor, disrupted Nov 2[4]

What changed this week

Edge appliances kept failing open. Ivanti's October fix was incomplete; only 25.1.1.3 and 22.8R2.6 close the UTA0576 chain, which ran in memory and evaded Ivanti's own integrity checker. SonicWall's SSL-VPN flaw entered KEV on Nov 6, and CISA's entry confirms it can bypass SAML-enforced MFA. Barracuda ESG got a public, near-complete root-cause write-up.[5][6][2][7]

Supply chains shifted from code to channels. cPGuard was hijacked through its billing portal and a stolen storage key; Cursor's marketplace served a trojanized Claude Code extension; DebugBear blames a registrar-level DNS change for the Polymarket drainer. In each case the payload was trusted because of where it came from.[1][8][9]

Secrets became the loot. Northflank says control-plane secrets were decrypted nine hours before detection; Chainalysis exposed every user's live tokens; Rails Active Storage could leak `secret_key_base` from an upload alone. Rotation, not patching, is the remediation.[10][11][12]

AI moved from headline to tooling. CERT-In names ARTEX, PentAGI and CyberStrikeAI in Crafty Falcon's attacks; WorkOS ties its breach to ARTEX user agents; Bitdefender suspects an automated retry loop in a school ransomware case. Treat these as assessments, but the defensive lesson is the same: faster attackers punish slow rotation.[13][14][15]

> **How to read this issue.** Each story separates **confirmed** (vendor, government, CVE/KEV record), **reported** (researcher or press, attributed) and **MAG212 analysis**. Corrections to our daily coverage are flagged in amber. IOCs are reproduced exactly as published and defanged. Commands state OS, shell, privilege and whether they change anything; none was executed by MAG212 on affected systems.

IN THIS ISSUE

Contents

START HERE
The week, day by day 04
Ten actions that matter now 05
KEV and patch tracker 06

01 · EDGE & REMOTE ACCESS
Ivanti: the patch that wasn't enough 07
PAN-OS cookie bug to ESXi 08
SonicWall SAML/MFA bypass 09
Barracuda ESG pre-auth root 10
Zyxel GS1900 & LXD 11
OpenSSH "SSHole" 12

02 · WEB & APPLICATION PLATFORMS
WordPress core & a dead plugin 13
PHP2Shell & GitLab 14
OFBiz, Rails, Drupal Commerce 15

03 · SUPPLY CHAIN & DEVELOPERS
cPGuard update hijack 16
Trojanized extension in Cursor 17
DebugBear & the PaaS breaches 18
Agent secrets & Chainalysis 19

04 · OT, IOT & RANSOMWARE
The cold chain 20
Node-RED on IoT2050 & XCPE 21
3AM, C3RB3R, Queens Library 22

05 · THREAT ACTORS & MOBILE
APT29's mobile watering holes 23
Android, Chrome & Crafty Falcon 24
SysGoRAT & help-desk to AD CS 25
NetamLoader, Binance, KELA 26

06 · AI, BREACHES & POLICY
AI security this week 27
Breach ledger 28

07 · DETECTION ENGINEERING
The week mapped to ATT&CK 29
Controls on trusted channels 30
Sigma rules: endpoint 31
Sigma rules: Linux, AD, web 32

DEFENDER'S TOOLKIT
Hunt pack: IOCs 33
Hunt pack: commands 34
Action desk by role 35
Awareness & next week 36
Verification & corrections 37
Source register 38

Get the daily and the weekly, free

Verified threats, the CVEs that matter, and the commands to act on them, in your inbox every morning and every Saturday.

Subscribe free → cyber.mag212.com/subscribe-free

TIMELINE · ALL DATES 2026

Seven days, forty stories

Key events by public disclosure date. Background items from the last days of October are shown where this week's coverage depended on them.

Oct 26–30 **Background.** PHP2Shell (CVE-2026-109618/-109619) in KEV Oct 26; Linux kernel CVE-2026-46300 KEV Oct 28 with a stated PHP-webshell-to-root chain; GitLab CVE-2026-97229 KEV Oct 29; Cursor serves trojanized Claude Code extension Oct 29; Polymarket drained via DebugBear script Oct 29; Ivanti CVE-2026-111357/-118527 KEV Oct 30; Northflank secrets decrypted Oct 30.[2][8][9][10]

Sun 1 FBI attributes the $6.3bn Binance theft to North Korea's TraderTraitor; GitLab federal deadline passes; Trigger.dev discloses env-var access.[16][2][17]

Mon 2 **cPGuard's update channel hijacked**: fake update runs as root 02:08–03:20 UTC. Google disrupts XCPE TV-box botnet. Android November bulletin. Barracuda advisory. Shadowserver: 1,000+ GitLab servers still vulnerable. Ivanti CVE-2026-111357 KEV due.[1][4][18][19]

Tue 3 KEV adds **WordPress CVE-2026-119977** (due Nov 6). Bitdefender details 3AM ransomware at a UK school estate. Chainstack and WorkOS disclose; KELA updates bank-phishing research. Binarly shows Zyxel exploit was a new bug. Chrome 157 stable.[2][15][20][21][22]

Wed 4 KEV adds **Apple CVE-2024-27834**; Sekoia publishes APT29 mobile watering holes. CERT-In issues Crafty Falcon advisory. Rails Active Storage GHSA. Siemens expands IoT2050 advisory to four models. Queens Library ransomware confirmed.[2][23][13][12][24][25]

Thu 5 US joint refrigeration fact sheet. OpenSSH "SSHole" disclosed and patched. watchTowr publishes Barracuda chain. OFBiz CVE records published. Check Point ChatGPT Lockdown bypass. OpenAI GPT-6 Cyber card. DOJ charges $129M deepfake fraud. Picus first-update-window analysis.[26][27][7][28][29][30][31][32]

Fri 6 KEV adds **SonicWall CVE-2026-19868** (due Nov 20). Chainalysis widens breach to all users. SSHole exploitation attempts. Northflank updates timeline. Japan adopts emergency cyber package. Apiiro agent-secrets research.[2][11][33][10][34][3]

Sat 7 SSHole attempts reach 11 IPs in 8 countries. CERT-In revises Crafty Falcon page. No KEV additions as of the Nov 6 catalog release.[33][13][2]

Pattern of the week. Five of the most serious incidents (cPGuard, Cursor, DebugBear, Northflank, SonicWall) required no user mistake. The victim's only "action" was trusting a channel that had already been compromised upstream.

PRIORITY LIST · RANKED BY EXPLOITATION AND BLAST RADIUS

Ten actions for Monday morning

#	If you run…	Status	Do this
1	Ivanti Connect Secure	Exploited · KEV	Capture memory and logs, then upgrade to **25.1.1.3** or **22.8R2.6**. Oct 13 builds are not enough. Rotate the LDAP bind account, LAPS passwords and BitLocker keys it could read.[6][5]
2	SonicWall Gen 7 / Gen 8 SSL-VPN	Exploited · KEV	Gen 8 → 8.2.3-8015; Gen 7 → newest 7.3.4 build. Hunt VPN logins with no matching IdP/MFA event. Due Nov 20.[35][2]
3	cPGuard on any server	Compromised	Update to ≥5.88.26, check the vendor IOCs, then rotate root password, SSH keys, MySQL root, S3/DO tokens and every host that trusts those keys.[1][36]
4	Cursor on macOS/Windows	Compromised	Check for Claude Code extension 2.1.312/2.1.313, the `svc-telemetry` key and LaunchAgent/SysMon task; run Cursor's remediation script; rotate host-reachable credentials.[8]
5	WordPress	KEV	Block `/wp-content/upgrade/`, confirm 403, update to 7.1.4 or branch fix, verify checksums. Delete (not deactivate) CryptoPayment Gateway.[37][32][38]
6	PHP / GitLab self-hosted	KEV	PHP ≥ 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12, restart every worker, patch kernel CVE-2026-46300, hunt webshells. GitLab: Oct 29 builds, then token rotation.[39][2][40]
7	Northflank, Trigger.dev, Chainstack, Chainalysis	Secrets exposed	Revoke at the issuer (AI, cloud, payment keys) before rotating in the platform; review provider logs from Oct 30.[10][11]
8	Alpine / musl SSH hosts	Attempts seen	Install branch-fixed `openssh` and restart sshd, or set `PasswordAuthentication no`.[27]
9	Barracuda ESG, LXD, OFBiz, Rails	Public detail	Patch before weaponization: ESG 9.4.0.029/030; LXD snaps; OFBiz 24.09.08; Rails 8.1.4.1/8.0.5.2 then rotate `secret_key_base`.[7][41][42][12]
10	Phones and TV boxes	Campaigns	MDM floor: current iOS, Android patch ≥ 2026-11-01, Chrome ≥ 157. Remove or isolate unmanaged Android TV boxes.[23][18][4]

Patching ≠ recovery. For Ivanti, cPGuard, Cursor, Northflank and Chainalysis, the update removes the attacker's path, not what they already took. Rotate first, then verify.

Evidence first. Ivanti's payload lived only in memory; SonicWall logs roll over on reboot. Capture memory and export logs before you patch or restart.

DATA · CISA KEV CATALOG VERSION 2026.11.06

What CISA confirmed as exploited

Added	CVE	Product	Due	Notes
Nov 6	CVE-2026-19868	SonicWall SonicOS SSLVPN	Nov 20	CWE-308; bypasses SAML-enforced MFA
Nov 4	CVE-2024-27834	Apple multiple products (WebKit PAC bypass)	Nov 18	Stage 2 of APT29 iOS chain (Sekoia)
Nov 3	CVE-2026-119977	WordPress Core	Nov 6	CWE-367; forensic triage: yes
Oct 30	CVE-2026-111357	Ivanti Connect Secure	Nov 2	Priv-esc; forensic triage: yes
Oct 30	CVE-2026-118527	Ivanti Connect Secure	Nov 13	Predictable upload location (CWE-340)
Oct 29	CVE-2026-97229	GitLab (Ruby/Onigmo regex)	Nov 1	Other Ruby products may be affected
Oct 28	CVE-2026-46300	Linux kernel	Oct 31	Chains with PHP2Shell to root
Oct 26	CVE-2026-109618/-109619	PHP runtime (“PHP2Shell”)	Oct 29	Fixed 8.2.35/8.3.36/8.4.27/8.5.12

No additions on Oct 31, Nov 1, 2 or 5. The catalog release read (2026.11.06, 19:44 UTC Nov 6) cannot show Nov 7 additions; re-check before closing tickets. Ransomware use is listed as “Unknown” for the three in-week additions.[2]

Notable patches and advisories, Nov 1–7

Vendor / product	Fixed version	Why it matters
Android (Nov bulletin)	Patch level 2026-11-01 / 2026-11-05	CVE-2026-58868 Framework RCE, no interaction; not known exploited[18]
Chrome 157	157.0.8103.38/.39	213 fixes, 7 critical; none flagged exploited (secondary source)[43]
OpenSSH / Alpine	10.6p2; Alpine branch packages	SSHole password bypass on musl, attempts observed[27]
Rails Active Storage	8.1.4.1 / 8.0.5.2 + mini_magick ≥5.1	CVSS 9.8 upload-triggered file read/write[12]
Apache OFBiz	24.09.08	46 CVEs; CVE-2026-83542 critical pre-auth RCE[42][28]
Barracuda ESG + 5 products	ESG 9.4.0.029 / .030 (sources differ)	Pre-auth root chain published Nov 5[7][44]
Siemens IoT2050	V4.3.4-1	Node-RED with no auth, CVSS 10, honeypot exploitation[24]
Microsoft Paint	11.2609.401.0 (Store only)	CVSS 8.1 RCE; Windows Update compliance won’t show it[45]
SonicWall GMS (EOL)	No fix	CVE-2026-109593/-109594; isolate and replace[46]
Cisco, WatchGuard	Per vendor (Nov 5)	UCS Central; WatchGuard Dimension unpatched for CVE-2026-98432[47]

Microsoft’s November Patch Tuesday falls on Nov 10, outside this window. No Apple security releases were published Nov 1–7.

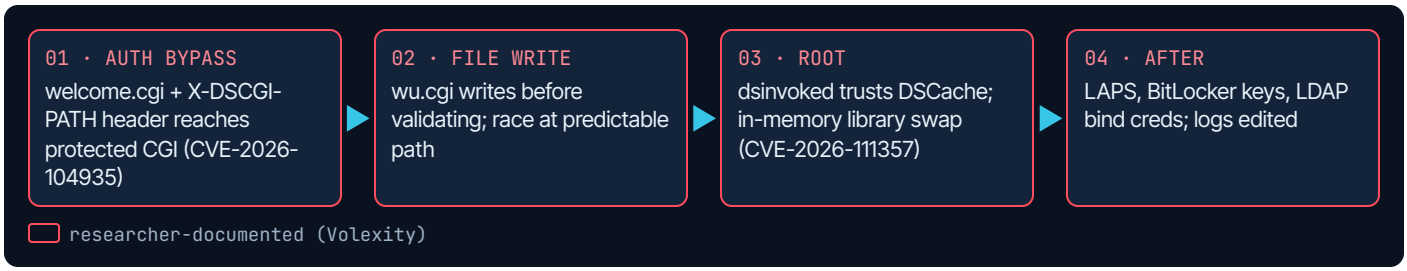
01 EDGE & REMOTE ACCESS

IVANTI CONNECT SECURE EXPLOITED · KEV

Ivanti: the October patch wasn't enough

Three bugs chained to unauthenticated root, a payload that lived only in memory, and an integrity checker that saw nothing. Only 25.1.1.3 or 22.8R2.6 closes the whole chain.

CVES	KEV DUE	FIXED	ACTOR
2026-104935 · -111357 · -118527	111357: Nov 2 · 118527: Nov 13	25.1.1.3 · 22.8R2.6	UTA0576 (Volexity)



Chain per Volexity. Mapping step 02 to CVE-2026-118527 is MAG212 inference from CISA's "known location on disk" wording; Volexity does not name that CVE. Diagram: MAG212 CYBER.[5][2]

What happened

Confirmed (KEV): CVE-2026-111357 (local privilege escalation) and CVE-2026-118527 (authenticated upload of attacker-controlled content "to a known location on disk") were added on Oct 30; each entry says it can be chained with the other two. **Reported (Volexity, Rapid7):** root on a 22.8R2.4 appliance from Oct 3; Ivanti says a "limited number of customers" were affected.[2][5][6]

The technical detail

The public `/dana-na/auth/url_default/welcome.cgi` is used to reach protected handlers because "the URL is used to determine whether the request is allowed, while the header path is used to determine the destination." A `wu.cgi` upload races execution against deletion at `/home/runtime/tmp/<MD5(filename)>`. The attacker then patched a library in memory and a DSCache task entry so the `dsinvoked` broker ran code as root, and restored both.[5]

Why the Integrity Checker missed it

No file on disk changed. Volexity says ICT "does not detect any modifications." The attacker also truncated `/home/runtime/dlogs/debuglog` and `/var/log/audit/audit.log` and ran a renamed tcpdump (`dsstatmond`) from hidden `/data/.icscap/`. A clean ICT result is not evidence of a clean box.[5]

Scores (they differ)

CVE-2026-111357: 8.8 (Ivanti) vs 7.0 (CVE record, Rapid7). CVE-2026-118527: 4.3. CVE-2026-104935: 8.6.[6]

Hunt

- WAF/proxy logs: bursts to `welcome.cgi`; any `X-DSCGI-PATH` header.
- IP `108.165.147[.]64`; files `/tmp/ml.py`, `/tmp/rq5.py`, `/data/.icscap/h.py`, `/home/lib/libdsplibs.so`.
- Full list: Volexity threat-intel GitHub, folder `2026/2026-10-13 Ivanti`.

Recover in this order

1. Preserve memory and logs before reboot.
2. Upgrade to 25.1.1.3 (or 22.8R2.6).
3. Investigate after patching; follow Ivanti recovery steps if compromise is suspected.
4. **MAG212:** rotate the ICS LDAP bind account, LAPS passwords and BitLocker keys it could read.

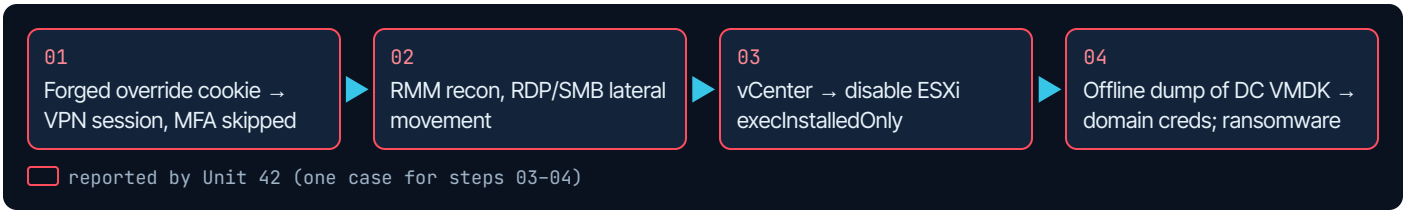
Correction: our Nov 1 edition gave a single "Nov 2" deadline; that applies only to CVE-2026-111357. CVE-2026-118527 is due Nov 13.

PALO ALTO PAN-OS GLOBALPROTECT RANSOMWARE

A cookie bug that ends at your hypervisor

CVE-2026-0257 is a May bug in GlobalProtect's authentication-override cookies. Unit 42 now ties it to Qilin and Inc ransomware, including a path from VPN to vCenter to an offline dump of a domain controller's virtual disk.

CVSS	KEV	WEAKNESS	NEW THIS WEEK
7.8 (v4.0, Palo Alto)	May 29 · ransomware: Known	CWE-565 cookie integrity	No vendor update



Per Unit 42 (updated Oct 26). Dumping a VM disk offline "bypasses in-guest EDR." Diagram: MAG212 CYBER.[48]

Am I exposed?

Confirmed (Palo Alto): a portal or gateway with authentication-override cookies enabled plus "a specific certificate configuration" the advisory does not detail. Check:

- Network › GlobalProtect › Portals › [portal] › Agent › [config] › Authentication: "Generate/Accept cookie for authentication override."
- Network › GlobalProtect › Gateways › [gw] › Agent › Client Settings › Authentication Override: "Accept cookie…"

Panorama and Cloud NGFW are not affected.[49]

Fixed versions

12.1.4-h6, 12.1.7; 11.2.4-h17, 11.2.7-h14, 11.2.10-h7, 11.2.12; 11.1.4-h33 … 11.1.15; 10.2.7-h34 … 10.2.18-h6 (see advisory table). Users re-authenticate once; cookies are regenerated with an HMAC.[49]

Fix without breaking cookies

Upgrade every portal and gateway that generates or accepts cookies together. Or bind override cookies to a **dedicated certificate** used for nothing else, or disable the feature. During phased upgrades the advisory documents `set global-protect enable-auth-override-cookie-hmac no` as a temporary, weaker setting; set it back to `yes` when done.[49]

Hunt (Unit 42 indicators)

- Successful GlobalProtect logins from `23.128.228[.]6`, `146.19.216[.]119/120/125`, `179.43.172[.]213`, `185.195.232[.]139` and others in the report.
- Host IDs `aa:bb:cc:dd:ee:ff`, `00:11:22:33:44:55`; device names `WINDOWS-LAPTOP-001`, `DESKTOP-GP01`, `GP-CLIENT`.
- PoC fingerprint: `Microsoft Windows 10 Pro 64-bit` with an empty user domain.
- GlobalProtect mapped onto management interfaces (TCP 4443, 3879).

If you get a hit

MAG212: end all GlobalProtect sessions; treat AD as compromised (krbtgt double reset, privileged rotation); rotate vCenter and ESXi root; re-enable and verify `execInstalledOnly` on every host; patch Veeam (CVE-2023-27532 was chained).[48]

Correction: our Nov 1 edition printed CVSS 9.1; Palo Alto's score is 7.8 (CVSS 4.0). KEV added it May 29, not May 13.

SONICWALL SONICOS SSL-VPN EXPLOITED · KEV

SonicWall: a second login path that skips SAML and MFA

CISA's Nov 6 KEV entry settles what the vendor's notes left vague: valid credentials for an alternate authentication method can bypass SAML controls and the MFA they enforce.

CVE	KEV	AFFECTED	FIXED
CVE-2026-19868 · CWE-308	Nov 6 · due Nov 20	Gen 7 ≤7.3.3-7015 · Gen 8 ≤8.2.2-8015	Gen 8 8.2.3-8015 · Gen 7 7.3.4

Confirmed (CISA KEV)

The flaw "may allow a user with valid credentials for an alternate authentication method to bypass SAML authentication controls. Successful exploitation may also bypass SAML-enforced multi-factor authentication (MFA)." Ransomware use: unknown.[2]

Update to our Nov 7 daily: we said no source confirmed the SAML/MFA detail; CISA's entry now does. The credential prerequisite matters: this is a stolen-password-plus-bypass threat, not an anonymous one.

Which build

Gen 8: 8.2.3-8015. Gen 7: SonicWall lists 7.3.4-7013 or later, but the 7013 release notes list no security fixes and 7.3.4-7015 was scheduled Nov 5; install the newest 7.3.4 build. Gen 7 NSv 7.3.4 was "not yet released" in the 7013 notes. Gen 6 is end-of-support.[35][50]

Same advisory, more holes

The 8.2.3 notes also fix a pre-auth SSL-VPN heap overflow, pre-auth TACACS+ heap and stack overflows, a session-validation flaw and weak password hashing.[50]

Hunt: VPN sessions without a second factor

For SAML users, a firewall VPN login with no IdP sign-in for the same user within minutes. For RADIUS/OTP users, no OTP success. Expect noise from clock skew and UPN vs sAMAccountName mismatches.

Harden while you patch

- Remove SSL-VPN authentication methods and local users you don't need.
- Restrict SSL-VPN by source (Geo-IP, allow-lists).
- Forward logs off-box before rebooting.
- Keep management off the WAN.

Also: GMS will not be fixed

SonicWall will not patch end-of-life GMS for CVE-2026-109593 (critical unauthenticated file read) or CVE-2026-109594 (SQL injection). Isolate and replace.[46][47]

READ-ONLY · SIEM · pseudo-query · field names are placeholders

```
SELECT v.time, v.user, v.src_ip, v.auth_method FROM firewall_vpn_logins v
LEFT JOIN idp_mfa_success m ON lower(m.user)=lower(v.user)
  AND m.time BETWEEN v.time - INTERVAL '5' MINUTE AND v.time + INTERVAL '5' MINUTE
WHERE v.time > TIMESTAMP '2026-10-20' AND m.user IS NULL;
```

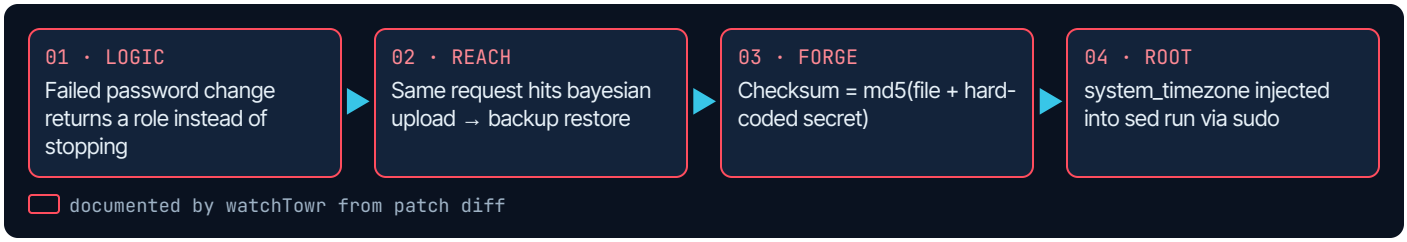
Logic illustration, not a product query. Map SonicOS syslog fields from your own samples. Not executed by MAG212.

BARRACUDA EMAIL SECURITY GATEWAY PUBLIC ROOT CAUSE

Barracuda ESG: from a failed password change to root

watchTowr's Nov 5 write-up spells out a four-step pre-auth chain. There is no known exploitation and no KEV listing, but the post is close to a recipe.

CVES	ADVISORY	ESG FIXED	EXPLOITED?
2026-116606 (9.3) · -111560 (8.6)	Nov 2	9.4.0.029 or .030 (sources differ)	No reports · not KEV



Chain per watchTowr (diff of 9.4.0.027 vs 9.4.0.029). Diagram: MAG212 CYBER.[7]

Step by step

1. An unauthenticated multipart POST to `/cgi-mod/index.cgi` with `user`, `new_password` and `retype_password` fails the change, but `_process_params` returns `$userrole` without stopping. The response is HTTP 200 with `"success":"true"`.

2. The same request carries `pu_bayesian_upload=1` and a file field `bayesian`, reaching `bayesian_upload_handler`, which rejects only `guest` and calls `Backup2::restore_all`.

3. Backups are tars with `backup.xml`; each file's checksum is `md5(bytes + secret + ".")` with the hard-coded secret "Barracuda Networks is your new best friend," so forged backups validate.

4. The restored `system_timezone` reaches a backtick `sed` in `fix_tz.pl`, run via `/usr/bin/sudo`, writing `/etc/sysconfig/clock`: root. The fix adds a `/usr/share/zoneinfo/` existence check and stops on the failed change.[7]

Scope

CVE-2026-111560 (root command injection) also affects Load Balancer ADC, Message Archiver, WAF Control Center, WAF and Web Security Gateway, where admin access is required; on ESG the bypass supplies it.[44]

Detect (MAG212, from the write-up)

- Unauthenticated POSTs to `/cgi-mod/index.cgi` containing both `new_password` and `pu_bayesian_upload`.
- Unexpected configuration-restore events.
- A `system_timezone` or `/etc/sysconfig/clock` value that isn't a valid zoneinfo name.

Remediate

Restrict the admin UI to trusted networks; confirm the patch under ADVANCED › Firmware Update › Firmware Patches; re-enable auto-patching; if compromise is suspected, work with Barracuda and rotate every credential the appliance held. watchTowr released a detection artefact generator, not an exploit; run it only against appliances you own.[44][7]

ZYXEL GS1900 SWITCHES EXPLOITED

Zyxel: "patched for KEV" switches are still exploitable

Reported (Binarly, Nov 3): the exploit behind the Kapibala switch hacks "was not CVE-2026-7273," the June bug CISA listed, but a separate flaw, CVE-2026-107441. `dispatcher.cgi` copies every POST parameter into a fixed global buffer without checking size or count; a long value overwrites the parameter counter and then function pointers, giving root command execution. The same pattern exists in `httprestorecfg.cgi` and `httpupload.cgi`, and the June check ran after the unsafe copy.[22][51]

Status: fixed only in firmware 2.90 Patch 3 (version strings ending `.3)C0`, 10 models); no workaround.

CVE-2026-107441 is **not** in KEV as of the Nov 6 catalog; CVE-2026-7273 is. ThaiCERT issued an alert Nov 6.[2][51]

Campaign (GreyNoise, Sept): 996 switches in 48 countries; 564 used default credentials; accounts `kapibala` / `kapibala2`, files `info.txt` and `c` in web paths, domain `*.981666.xyz`, outbound TFTP from switches.[51]

Recover

Inventory firmware strings; move web management to a management VLAN; install Patch 3; rotate admin, SNMP and RADIUS/TACACS+ secrets. Where defaults were used or management was exposed before Patch 3, factory-reset and rebuild from a known-good config.

READ-ONLY · Linux/macOS · curl · from a NON-management segment

```
curl -sk -o /dev/null -w "%{http_code}\n" --max-time 5 https://<switch-ip>/
```

Any code other than `000` means the web UI is reachable from that segment. Not executed by MAG212.

CANONICAL LXD / MICROCLOUD PUBLIC POC

LXD: a public certificate was enough to become a trusted client

Confirmed (Canonical, Oct 28): LXD's remote API mTLS check "checked all certificates the client sent against the trust store, not just the leaf." Because "only the leaf certificate proves ownership of the signing key," anyone holding a trusted client's *public* certificate could authenticate as it, "depending on the privilege of the victim user," up to host root. MicroCloud joins are affected too. No workaround.[41]

Fixed (snap stable from Oct 29): LXD 6.10.1, 5.21.9, 5.0.11, 4.0.15; MicroCloud 3.4.1, 2.1.5. CVE-2026-112816, CVSS 4.0 10.0 from Canonical as CNA (via Rescana). A public lab reproduction tool appeared on GitHub Nov 1. Not in KEV; no exploitation reported. Ubuntu archive `lxd` debs are not affected.[41][52]

MAG212: rotating client certs doesn't help (the attack needs only the public half); patching does. After patching, review the trust store for entries added before the fix.

READ-ONLY (first three) · Linux · lxd group or root

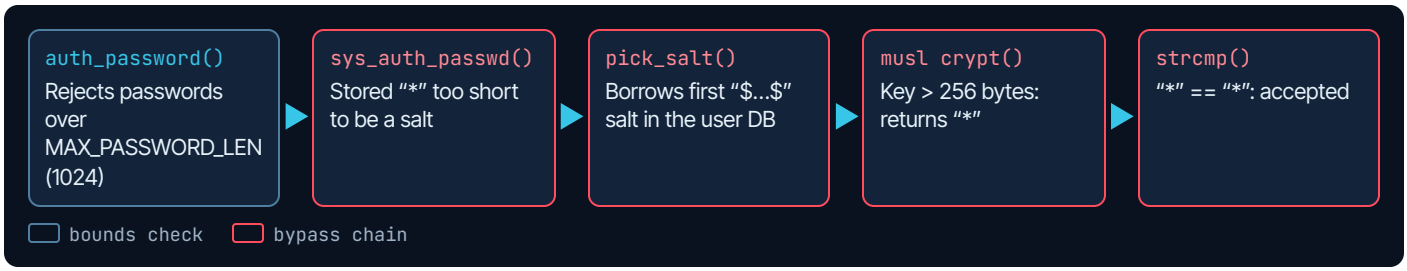
```
snap list lxd microcloud
lxc config get core.https_address      # empty = no network listener
lxc config trust list
sudo snap refresh lxd                  # CHANGE: applies the fix (per Canonical)
```

Also check `cluster.https_address` on clusters; default API port is 8443. Not executed by MAG212.

OPENSSH ON MUSL (ALPINE) ATTEMPTS SEEN

SSHole: how a 257-byte password matches "*"

Disclosed and patched Nov 5. By Nov 7, Previdian's sensors had logged 17 attempts from 11 IPs in 8 countries. Not in CISA KEV.



From OpenSSH-portable source and Alpine's advisory. Linking pick_salt() to the "5/6" condition is MAG212's reading of the code. Diagram: MAG212 CYBER. [53][54][27]

Exposure conditions (Alpine)

- sshd without PAM, or `UsePAM no`.
- `PasswordAuthentication yes` (default).
- A reachable account whose password field is `*`, e.g. `root:*`, key-only users, tiny-cloud's `alpine` user (images 3.18.11–3.24.3).
- At least one local `$5$` / `$6$` hash. One password-holding user exposes every `*` account.

Root needs `PermitRootLogin yes` or a path such as `doas`. [27]

The week's telemetry

Nov 6: 8 attempts from one IP in Japan (The Hacker News). Nov 7: 17 attempts, 4 sensors, 11 IPs in CH, DK, IR, JP, NL, NO, SG, US. Previdian's CEO says attackers ran `id`, `uname` and `hostname` after a honeypot root login; no logs are public. "Previdian KEV" is the company's own list, not CISA's.[33]

Fixed packages

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. Restart sshd. Upstream OpenSSH 10.6p2 adds a workaround.[27]

READ-ONLY · Alpine · ash · root · prints names only

```
awk -F: '$2=="*"{print $1}' /etc/shadow            # bypass targets
awk -F: '$2 ~ /^\$[56]\$/{print $1}' /etc/shadow    # salt donors
grep 'Accepted password for' /var/log/messages*
sshd -T | grep -Ei '^(usepam|passwordauthentication|permitrootlogin) '
```

Both awk lines returning names with password auth on = Alpine's exposure conditions. Not executed by MAG212.

CHANGE · Alpine · root · from Alpine's advisory

```
apk upgrade -U -a && rc-service sshd restart
# stopgap: echo 'PasswordAuthentication no' > /etc/ssh/sshd_config.d/00-no-passwords.conf
```

Confirm key login works first; keep an existing session open.[27]

02 WEB & APPLICATION PLATFORMS

WORDPRESS CORE KEV

WordPress: the update race, and a plugin you must delete

CVE	AFFECTED	KEV	CVSS
CVE-2026-119977 · CWE-367	4.7.0 – 7.1.3 (CNA)	Nov 3 · due Nov 6 · triage	8.1 (Wordfence CNA)

Confirmed

KEV: unauthenticated code execution "during the upgrade window… due to predictable, web-accessible staging paths used during full-package core upgrades," with forensic triage required. The CVE record (Wordfence CNA) settles the affected range at 4.7.0–7.1.3; WordPress.org says backports go "through 4.7" but publishes no per-branch table. There is no 7.1.5.[2][37][55]

What we learned this week

Picus (Nov 5): the first upgrade that installs the fix runs the *old* extraction code, so the random staging name and protective `index.php` only arrive with the next update; the new `update-core.php` still blocks the config swap. Block the path in the root `.htaccess`, not inside the upgrade folder, and don't treat `wp core update` as a safe substitute.[32]

Wordfence via The Hacker News (Nov 6): attempts within nine minutes of its rule deploying; lab tests show the window lasts "only seconds."[56]

Branch	7.1	7.0	6.9	6.8	6.7	6.6	6.5	6.4	6.3	6.2	6.1	6.0
Fixed	7.1.4	7.0.8	6.9.11	6.8.12	6.7.11	6.6.11	6.5.14	6.4.14	6.3.14	6.2.15	6.1.16	6.0.18

Next point release after the CNA's last affected version; older branches follow the pattern down to 4.7.39. MAG212 derivation.[37]

READ-ONLY · Linux · Bash/WP-CLI · site owner / root for logs

```
curl -s -o /dev/null -w '%{http_code}\n' https://<site>/wp-content/upgrade/x.php   # expect 403 before updating
sudo zgrep -E '/wp-content/upgrade/[^" ]*\.php' /var/log/nginx/access.log*
wp core verify-checksums && wp user list --role=administrator --fields=ID,user_login,user_registered
```

Not executed by MAG212.[57]

CRYPTOPAYMENT GATEWAY PLUGIN NO FIX · CVSS 10

Why "deactivate" is not enough for CVE-2026-81648

Confirmed (WPScan CNA): slug `cryptopayment-gateway`, versions 1.2.1–1.2.2, CVSS 10.0, CWE-862, no fix. The flaw is a standalone, unguarded router at `vendor/cryptd/ajax.php` with actions `get-settings`, `save-settings`, `encryption` and `delete-file`: unauthenticated settings overwrite, arbitrary file deletion and cleartext wallet-credential recovery.

CISA's enrichment rates exploitation "poc"; attempts in the wild are reported by Defused Cyber.[38]

MAG212 analysis: because `ajax.php` is a plain PHP file under `wp-content/plugins/`, the web server executes it on direct request whether or not WordPress loads the plugin. Deactivation does nothing; deletion does. Treat wallet keys as exposed on any site that ran these versions.

CHANGE · WP-CLI · site owner

```
wp plugin deactivate cryptopayment-gateway && wp plugin delete cryptopayment-gateway
sudo zgrep -E 'cryptopayment-gateway/vendor/cryptd/(ajax|upload)\.php' /var/log/nginx/access.log*   # read-only
```

`wp plugin delete` removes files without running uninstall hooks, so deactivate first. Then check gateway wallet addresses and `wp-config.php`, and rotate wallet keys. Not executed by MAG212.[58][38]

PHP RUNTIME KEV · BACKGROUND

PHP2Shell: patch PHP, then patch the kernel

Confirmed: "PHP2Shell" is CVE-2026-109618 ("RCE via OOM corruption") and CVE-2026-109619 ("RCE via stale global state") in PHP itself. KEV added both Oct 26 (due Oct 29, forensic triage). Fixed in **8.2.35, 8.3.36, 8.4.27, 8.5.12.** Both CVE records were updated Nov 5; what changed is not stated.[2][39]

Mechanism (CVE text): PHP uses `longjmp()` for out-of-memory errors; some contexts leave request memory uninitialized and cleanup later reads or branches on it. Separately, global state can keep pointing into freed request memory. **Reported (Recorded Future):** a use-after-free in the session upload-progress unserializer (enabled by default since PHP 5.4) and an OPcache type confusion; Wiz showed RCE on WordPress, Drupal and Joomla; leaked details hit VirusTotal hours before the fix.[39][59]

Why it's in the weekly: KEV's Oct 28 entry for Linux kernel CVE-2026-46300 says it "can be chained with CVE-2026-109618 and CVE-2026-109619 to implant PHP webshells and run commands as root." A host that patched PHP after a webshell landed, but not the kernel, can still be rooted.[2]

Interim hardening (relayed from PHP's advisory; none makes an install safe): `session.upload_progress.enabled=0` in php.ini or the FPM pool (not `.user.ini`), restart every worker; lower `post_max_size`; WAF-block multipart on sites that take no uploads.

READ-ONLY · Linux · shell · per SAPI

```
php -v; php-fpm8.3 -v 2>/dev/null      # CLI and FPM can differ; check phpinfo() per pool
php -i | grep -E 'session.upload_progress.enabled|post_max_size'
grep -RHn 'auto_prepend_file' /etc/php 2>/dev/null   # common webshell hook
```

Unit names vary by distro. After upgrading, `systemctl restart php8.x-fpm` (CHANGE). Not executed by MAG212.

GITLAB SELF-MANAGED KEV

GitLab: deadline passed, 1,000+ servers still exposed

Confirmed: CVE-2026-97229 (CVSS 10.0) lets an unauthenticated user run code via a crafted regular expression in a CI/CD configuration. KEV added Oct 29, due **Nov 1**, forensic triage required, and warns that "other products can potentially be affected by the same underlying Ruby/Onigmo Integer Overflow." Affected 19.2 <19.2.8, 19.3 <19.3.5, 19.4 <19.4.2.[2][40]

Reported (Shadowserver via BleepingComputer, Nov 2): over 1,000 instances still vulnerable, and about 11,300 vulnerable to sibling CVE-2026-110264, which is **not** in KEV, out of ~39,000 seen daily. The latest patch set (Oct 29: 19.5.3, 19.4.5, 19.3.7 and others) covers both.[19]

Signals (from our Oct 31 guide): Workhorse 502 / "failed to receive response: EOF," Puma worker crashes, `regexp_matcher.rb` in traces, requests to the CI lint endpoint.

READ-ONLY · Linux package install · root

```
sudo gitlab-rake gitlab:env:info
sudo gitlab-rake gitlab:tokens:analyze          # inventory before rotation
sudo zgrep -E 'ci/lint|regexp_matcher\.rb|failed to receive response' \
  /var/log/gitlab/gitlab-workhorse/* /var/log/gitlab/gitlab-rails/*
```

GitLab documents no Rake task that rotates tokens; rotate via UI or API. Not executed by MAG212.[60]

THREE PLATFORMS, THREE FIXES NO EXPLOITATION · EXCEPT DRUPAL

OFBiz, Rails and Drupal Commerce

Apache OFBiz 24.09.08: one of 46 stands out

Confirmed: 24.09.08 fixes 46 CVEs. The records published Nov 5 rate **CVE-2026-83542** critical (CISA enrichment 9.8): a multipart upload stages crafted widget XML, an anonymous JSON request overrides `mainDecoratorLocation` on a manager login route, and OFBiz evaluates an unsandboxed Groovy expression while rendering the login-failure page. The Nov 6 update adds that a request "kept in flight" suffices, nothing is written to disk, and the unauthenticated `/sfa/control/editPortalPageColumnWidth` route returns command output in an HTTP 200.[42][28]

Also "important": CVE-2026-68524 (temp-file descriptor + `file:` URI loads a Screen definition) and CVE-2026-73578 (`_LAST_VIEW_NAME_` saved-view state skips re-authentication). None in KEV; OFBiz has three earlier KEV entries (2024).[42][2]

MAG212: file-integrity monitoring won't see this. Watch web logs for the route and parameter names below and for a Java process spawning shells.

READ-ONLY · Linux · log read access

```
sudo zgrep -E '/sfa/control/editPortalPageColumnWidth|_LAST_VIEW_NAME_|mainDecoratorLocation'
/path/to/ofbiz/access*.log*
```

Markers derived from CVE text, not vendor IOCs. Not executed by MAG212.

Rails Active Storage: an upload alone can leak secret_key_base

Confirmed (GHSA-f3w6-w445-fwh9, Nov 4; CVE-2026-122006, CVSS 9.8): "ImageMagick chooses a coder based on the file's content, and some coders read or act on files named inside the image." The analyzer runs on attach, so no variant call is needed. Exposed if `variant_processor = :mini_magick` (default for `load_defaults 6.1` or earlier), the system ImageMagick policy doesn't deny the coders (Debian/Ubuntu defaults don't), and the app takes untrusted uploads.[12]

Fix: activestorage 8.1.4.1 or 8.0.5.2 with mini_magick ≥ 5.1. With Disk storage, rotate `secret_key_base` and every readable secret; "do not keep exposed secrets as fallbacks." Rotating `secret_key_base` logs users out and can affect signed URLs. GitHub's advisory still shows "No known CVE" because MITRE assigned it.[12][61]

READ-ONLY · app dir · deploy user

```
bundle list | grep -E "activestorage|mini_magick"
magick -list policy        # IM7; 'convert -list policy' on IM6 — MSL, gs, PS/PDF should be denied
bin/rails secret           # generates a new value; storing it is the CHANGE
```

Not executed by MAG212.

Drupal Commerce: exploited as fraud, not as a shell

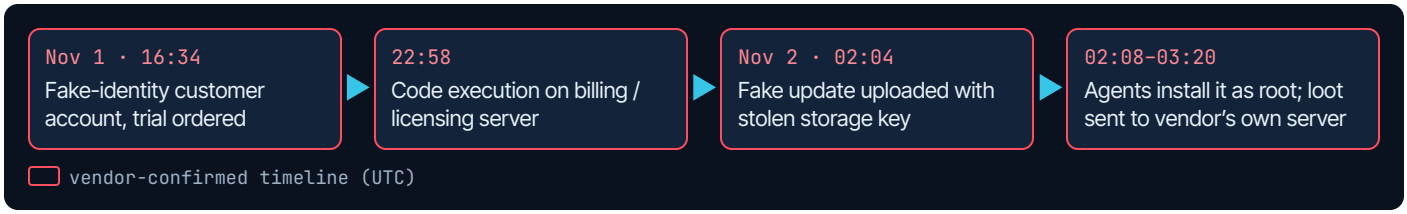
Confirmed (SA-CONTRIB-2026-254, Oct 28): access bypass, risk 21/25, "being actively exploited in the wild"; fixed in 3.3.13 and 8.x-2.41. Not in KEV; CISA's enrichment scores it 6.5 with exploitation "none," which conflicts with Drupal. **Reported (Centarro via Rescana):** unpaid orders, orders shown paid with no payment, prices changed to $0.01, unauthorized discounts; headless JSON:API sites hit by a different route. Patch, run `drush pm:security`, and reconcile orders since Oct 28.[62][63][64]

03 SUPPLY CHAIN & DEVELOPERS

CPGUARD (OPSSHIELD) COMPROMISED UPDATE

cPGuard: the security agent that ran the attacker's script as root

RAN FAKE UPDATE	WINDOW	AFFECTED	UPDATE TO
~2,950 servers	Nov 2, 02:08–03:20 UTC	5.88.12 – 5.88.19	≥ 5.88.26 (pages differ)



Per OPSSHIELD's Nov 3 disclosure. The exact request that gave code execution was not logged. Diagram: MAG212 CYBER.[1]

What the script did (confirmed)

Read `/etc/shadow`, `/etc/passwd`, `/root/.ssh` (private keys, `authorized_keys`, `known_hosts`), `/root/.my.cnf`, root shell history and, on some servers, `/root/.s3cfg`; left a setuid-root shell and a cron task; staged loot in `/var/tmp/.cpg91511/loot.tgz`. It exfiltrated to OPSSHIELD's licensing server under a compromised account. About 7,900 billing accounts (bcrypt hashes) were also exposed.[1][36]

Two numbers, don't merge them

~2,950 servers *ran* the update; the vendor's preliminary estimate is that the attacker *retrieved* 32 collected files. Plan rotation for the first number.[1][36]

Version conflict

The advisory says "5.88.25 or later"; the disclosure names 5.88.26 (removes the root shell) plus a follow-up that removes the cron task. Use ≥ 5.88.26.

Rotate in this order (vendor)

1. Update; confirm IOC files and cron entry are gone.
2. Change root and local passwords from a trusted recovery environment.
3. New root SSH keys; remove the old public keys everywhere.
4. MySQL root and `.my.cnf`; secrets in history, S3 keys, DigitalOcean tokens.
5. Treat every host reachable by those SSH keys as compromised until rekeyed.
6. Rebuild from a pre-Nov 1 backup if integrity can't be established.

Vendor IOC	Value (exact)
Script SHA-256 · i91511.sh	`2c2acd988da531d133d0e17f245c49bf15781278f837543d18c95e8410eabd38`
Script SHA-256 · i91511b.sh	`ffd7a47f65fa1244429baa936ae94be54676b53d2f88bc39564f24e22011de8a`
Script SHA-256 · i91511c.sh	`d73919af84bf46de941db85e27fd1abc65701ef9ce6cf33bb27c5397f4a41c26`
Script SHA-256 · i91511d.sh	`6add0201e9a3d02de772d561d05e0da86eb1c538686753b7adcc3aedf7366f77`
Customer-server files	`/etc/cron.d/i93677 · /var/tmp/.i93677/ · /var/tmp/.cpg91511_sh (setuid) · /var/tmp/.cpg91511/`
Operator IP · user agent	`94.183.188.91 · cPGuard/5.88.11`

READ-ONLY · Linux · bash · root

```
grep 'Successfully updated' /opt/cpguard/logs/install_log; cpgcli --version     # vendor commands
ls -la /etc/cron.d/i93677 /var/tmp/.cpg91511_sh /var/tmp/.cpg91511 2>/dev/null
find /var/tmp /tmp -xdev -perm -4000 -type f -ls
```

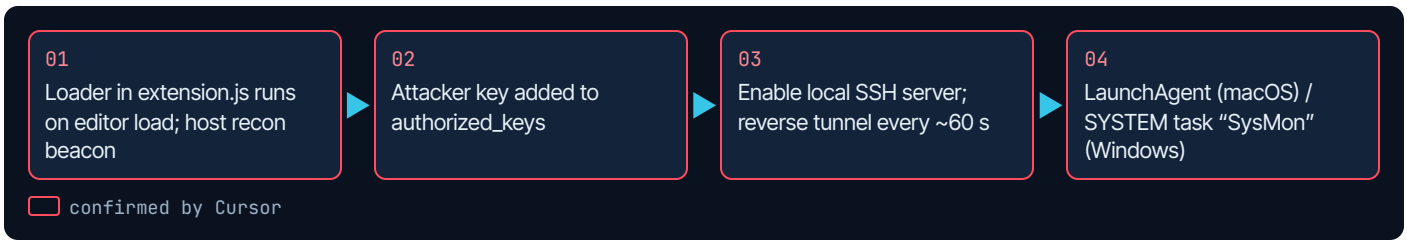
The vendor warns a negative result doesn't prove the script never ran. Not executed by MAG212.[36]

CURSOR MARKETPLACE COMPROMISED EXTENSION

The "Claude Code" extension that opened an SSH tunnel

For eleven hours on Oct 29, Cursor's marketplace served trojanized builds of an extension named Anthropic.claude-code, "not developed by Anthropic," per Cursor. Reuters quoted Cursor: up to 5,000 users.

VERSIONS	PLATFORMS	LIVE	ROOT CAUSE
2.1.312 · 2.1.313	macOS arm64 · Windows x64	Oct 29, ~02:27–13:35 PT	Not disclosed



Admin-only steps "usually fail without admin rights"; the attacker server is offline. Diagram: MAG212 CYBER.[8][65]

Indicator (Cursor)	Value (exact, defanged)
Payload extension.js SHA-256	`ecb58cb29078d9646ad1dcdbe51526f2d9cfea06be5fb2ab183e8ecc3ab6bf15`
VSIX 2.1.312 darwin-arm64	`fcbb327e38e61c4fec795e0d0591f52cd1014b813d20a5912104953c3a17c364`
VSIX 2.1.312 win32-x64	`3de1722901165769893bef57c72594e9a54459faa23f3091b136b79966edd081`
VSIX 2.1.313 darwin-arm64	`80402fdcad8799285fd93044976973ca000da7995fb93363f819bb8e4f84ee6c`
VSIX 2.1.313 win32-x64	`6786ec90cbd45949695bd7805c9fbb26cfc91bc5fc897de0183d9bcb9cb21731`
Host · beacon · tunnel	`134[.]209[.]82[.]225 · POST :8099/beacon · ssh user "tunnel" on TCP 22`
SSH keys	`comment svc-telemetry · SHA256:0Z6R+DF64Do2nwQic8a7kkfDLNNk4IiK+2U2Rci4htk · tunnel key SHA256:KOAU57+ZG6u3MG4WwzPzPX2O5YEe9qdOC1Bl+6MVyDQ`
macOS files (Linux: /tmp/.stk_*, cron @reboot)	`~/.config/.smt · ~/.config/.smtk · $TMPDIR/.stk_<10 hex> · ~/Library/LaunchAgents/com.apple.sysmond.plist`
Windows files	`%USERPROFILE%\.config\smt.cmd · %USERPROFILE%\.config\smtk · %TEMP%\.stk_<10 hex> · task SysMon · Startup\sysmon.cmd`
Command lines	`ssh -N -R '*:0:localhost:22' · autossh -M 0 · StrictHostKeyChecking=no · UserKnownHostsFile=/dev/null · ExitOnForwardFailure=yes`

READ-ONLY · macOS/Linux · bash · affected user

```
cursor --list-extensions --show-versions | grep -i claude-code
ssh-keygen -lf ~/.ssh/authorized_keys | grep -E 'svc-telemetry|0Z6R\+DF64Do2nwQic8a7kkfDLNNk4IiK'
ls -la ~/Library/LaunchAgents/com.apple.sysmond.plist ~/.config/.smt ~/.config/.smtk; launchctl list |
grep sysmond
```

Flags per VS Code CLI docs (Cursor is a fork; also inspect the extensions folder). Match keys by fingerprint. Windows: search `$HOME\.ssh\authorized_keys` and `C:\ProgramData\ssh\administrators_authorized_keys`. Not executed by MAG212.[66][8]

Clean up: run Cursor's `remediate-macos.sh` as the affected user (not root) or `remediate-windows.ps1` from an Administrator PowerShell; both exit non-zero if anything remains. Uninstalling alone may not be enough. Then rotate every credential reachable from the machine, from a trusted system.[8]

MAG212: hunt the reverse-tunnel command line and outbound TCP 22/8099 to the host above for Oct 29–30. Headless CI using the npm CLI is not implicated.

THIRD-PARTY SCRIPT · PAAS SECRETS FOURTH-PARTY RISK

A DNS change drained traders; PaaS vaults leaked keys

DebugBear → Polymarket

Reported (The Hacker News, BleepingComputer): on Oct 29 a DebugBear real-user-monitoring script on Polymarket, `cdn.debugbear[.]com/C7xcKKrjUnXK.js`, was swapped for a drainer. It read browser-stored account details and trading API keys, found the order code and signer, and either moved wallet-login users' positions to the attacker or sold email-login users' positions at worsening prices, all signed with the victim's own signer and submitted by Polymarket's relayer. About 28.6M POL (~$2.6M) went to `0x3F99139F1C5854bb628c2e576Aaf638e99dFfc18`; C2 was `data.debugbear.com`.[9][67]

New this week: DebugBear says its "DNS records were compromised via its registrar," with no sign of intrusion into its systems and one customer apparently targeted; a researcher says the registry record changed ~9 minutes before the attack. Polymarket returned $3.9M ($2.7M to 726 wallets, $1.19M for the trading pause) and plans stronger CSP, pinned versions and sandboxing.[9]

MAG212: SRI is impractical for a vendor-updated RUM script, so isolate it: no third-party script should share an origin with a signer or session token. CSP `report-to` logs reveal what third-party hosts actually load.

Northflank, Trigger.dev, Chainstack, WorkOS

Platform	What was exposed (confirmed unless noted)	What to do
Northflank	Control-plane secrets decrypted from **02:39 UTC Oct 30**, ~9 hours before Wiz's alert; "assume all environment variables were decrypted." Patched "CVE-2026-98432" fleet-wide; RCA pending.[10]	Rotate in order: AI keys, cloud, payment, private keys, DB creds. Reconnect VCS and IAM roles.
Trigger.dev	"Unauthorized access to environment variables" for a subset of orgs; exploit blocked; no dates or mechanism published.[17]	Treat all env vars as exposed; follow emailed steps.
Chainstack	Dev Oct 26 → prod Oct 29 via a third-party component; names, emails, password hashes; node-credential systems accessed. Closed Nov 2.[20]	Change passwords, rotate node credentials and platform API keys.
WorkOS	Internal sales app (CRM, call/support/Slack summaries). **Reported:** attacker used ARTEX AI; user agents `artex-enrich/1.0`, `norma/0.4`.[68][14]	No secrets to rotate; expect convincing phishing built from real threads.

SecurityWeek reports the incidents do not appear related.

READ-ONLY / CHANGE · AWS CLI · IAM admin

```
aws iam list-access-keys --user-name <user>                                  # read-only
aws iam update-access-key --user-name <user> --access-key-id <id> --status Inactive   # CHANGE, after replacement is live
grep -rn "debugbear" ./src ./public ./dist 2>/dev/null                       # find leftover embeds
```

Revoke at the issuer first (AI provider, cloud, payment), then update the platform and redeploy. Not executed by MAG212.

SECRETS AT REST RESEARCH · BREACH

“Don’t ask again” files and Chainalysis tokens

Coding-agent approval files

Reported (Apiiro via The Hacker News, Nov 7): 1,122 of 104,185 public `.claude/settings.local.json` copies held secrets: 1,379 distinct, including 379 database passwords, 43 SSH logins, 42 GitHub/GitLab/npm tokens and 23 AWS keys. 734 more sat in deleted versions; 211 forks of 74 repos carried them. gitleaks caught 564 files, TruffleHog 643, neither 215. Validity wasn’t tested.[3]

Confirmed (Anthropic docs): “Yes, and don’t ask again” writes an `allow` rule into that file; the first write in a repo adds `**/.claude/settings.local.json` to the user’s **global** git excludes, not the project `.gitignore`. Teammates, hand-made files and already-committed files are not covered. No Anthropic response has been reported.[69][3]

Chainalysis

Confirmed (company): an Oct 30 incident widened on Nov 6 to names, usernames, password hashes and **live tokens for all users**; KYT, address screening, Reactor and Data Solutions went offline or locked; the company describes “offensive agentic techniques” without published evidence. Latest update (Nov 6, 03:30 EST): KYT and address screening returning in phases behind IP allowlisting; Reactor and Data Solutions still offline. No Nov 7 entry.[11]

Do: reset passwords, rotate API keys after allowlisting, find every system storing a Chainalysis key, review API logs from Oct 30, and document interim screening for compliance.

READ-ONLY · Git · authorized full clone

```
git ls-files -- '.claude/*' '.cursor/*' '.gemini/*' '.specstory/*'
git log --all --format='%h %ad %an' --date=iso-strict -- '.claude/*'
git check-ignore -v .claude/settings.local.json
```

Lists paths and metadata only; never print the contents into tickets. Not executed by MAG212.

CHANGE (adds file) · .gitleaks.toml · gitleaks v8

```
[extend]
useDefault = true
[[rules]]
id = "inline-cli-password"
regex = '''(?i)(?:--password[= ]|PGPASSWORD=|MYSQL_PWD=)([^\s'"]{6,})'''
secretGroup = 1
[[rules]]
id = "credential-in-url"
regex = '''[a-z][a-z0-9+.-]*://[^:/\s@]+:([^@/\s]{4,})@'''
secretGroup = 1
```

Starting point, expect false positives. Scan history with redaction: `gitleaks detect --source . --log-opts="--all" --redact --config .gitleaks.toml`. Not executed by MAG212.

> **The common thread.** Approval files, PaaS env stores, a security agent’s root context, a trading front-end: this week’s attackers went where secrets already sit decrypted. Inventory those places as part of your attack surface, and make rotation a rehearsed procedure, not an incident-day improvisation.

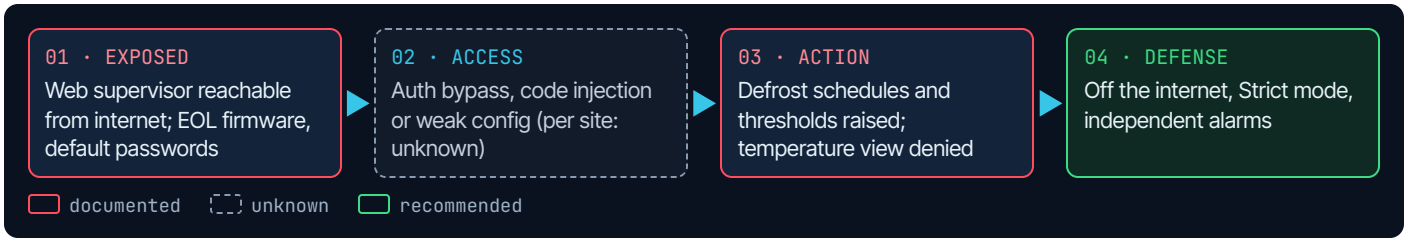
04 OT, IOT & RANSOMWARE

REFRIGERATION CONTROLLERS GOVERNMENT WARNING

The cold chain: an exposure problem, not a zero-day

Four weeks of defrost-forcing attacks in European supermarkets, a French blood-service incident on Nov 2, and on Nov 5 a five-agency US fact sheet. No CVE, port or IOC has been tied to the 2026 attacks.

US FACT SHEET	ISSUERS	CERT-FR	NAMED GEAR
Nov 5 · TLP:CLEAR	CISA · FBI · HHS · USDA · DoT	ALE-012 · Oct 12–16	Danfoss AK-SM/AK-SC · Dixell/Copeland xweb



Steps per the US fact sheet and CERT-FR. Diagram: MAG212 CYBER.[26][70]

Confirmed (US fact sheet)

Attackers exploit "unpatched or internet-accessible" electronic temperature and commercial refrigeration controllers via authentication bypass, arbitrary code injection and weak configuration, forcing "continuous heating and defrost cycles" and denying operators a view of temperatures. Mitigations are mapped to CISA's cross-sector goals: no internet exposure for controller panels, a dedicated OT VLAN, changed default passwords and phishing-resistant MFA, firmware and end-of-life lifecycle, device/IP allowlists for config changes, offline backups, logging or packet capture, and alerts on setpoints outside safe ranges.[26]

Confirmed (CERT-FR)

Names Danfoss AK-SC and AK-SM, Copeland xweb and Dixell xweb. If not compromised: remove internet exposure, review the full configuration **including defrost schedules**, allow access only over VPN, and set Danfoss units to **Strict**. If compromised: restart Danfoss units, factory-reset others, reconfigure before reconnecting. Exposing end-of-life equipment means "a very high probability of compromise."[70]

Exposure (Oct 15, background)

About 350 Danfoss AK-SM 800A online (down from 550+); 2,900–5,200+ StoreView panels; 1,173 Copeland XWEB units. Danfoss says most affected units were older models no longer updated.[71]

What "defrost forcing" means (MAG212)

Defrost is a scheduled mode that energizes heaters or hot gas and suspends cooling. Rewriting schedules and alarm limits through the web supervisor turns cooling into heating while keeping alarms quiet. That's why CERT-FR singles out defrost review, and why EFS kept its plasma: alarms outside the vendor channel still fired.[72]

Verify

Diff defrost schedules, setpoints and alarm limits against a known-good export; confirm from outside that the supervisor doesn't answer on your public IPs; test that alarms reach on-call staff without the vendor portal.

SIEMENS SIMATIC IOT2050 CVSS 10 · EXPLOITED IN HONEYPOTS

An open Node-RED editor is a root shell

CVE	ADVISORY	MODELS	FIXED
CVE-2026-58115 · CWE-306	SSA-834709 V1.1 · Nov 4	Advanced · Basic · M.2 · SM	V4.3.4-1 or later

Confirmed (Siemens): "Affected devices do not enforce authentication on the Node-RED HTTP interface"; an unauthenticated attacker can create flows that run code with maximum privileges. V1.1 expanded the list to four models (6ES7647-0BA00-1YA2, -0BA00-0YA2, -0BB00-1YA2, -0CA00-1AA2). Workarounds: uninstall Node-RED or harden it per the Node-RED guide.[24][73]

Reported (VulnCheck via The Hacker News): honeypot exploitation since Oct 30 using flows with an HTTP-in endpoint, a function node and an exec node. Stage 1 fetches an AMD64 bot from `85.215.73[.]250` to `/dev/shm/.b`; stage 2 fetches `wget.sh` and `.sys_update` from `45.194.90[.]57:38472` to `/tmp/.kworker`. A backdoor variant wires an HTTP endpoint straight to exec, surviving reboot because flows persist on disk.[74]

READ-ONLY · any shell · from an engineering host / device root for files

```
curl -s http://<iot2050>:1880/auth/login          # {} = no adminAuth configured
ls -la /dev/shm/.b /tmp/.kworker 2>/dev/null
grep -c '"type":"exec"' ~/.node-red/flows*.json     # path varies; review every exec node
```

TCP 1880 is Node-RED's default. Fix: update to V4.3.4-1; until then set `adminAuth` (bcrypt) and `httpNodeAuth` in settings.js, block 1880, delete unknown exec/http-in nodes, rotate credentials stored in flows, and reimage confirmed victims. Not executed by MAG212.

ANDROID TV BOXES BOTNET DISRUPTED

XCPE: a backdoor that shipped from the factory

Reported (BleepingComputer on Google GTIG, Nov 2): Google, Japan's National Police Agency and partners disrupted XCPE, preinstalled on 1.3M+ Android TV boxes and attributed to OEM Videostrong, which Google banned from certified Android. Components `x.cpe` and `com.oemservice` run as system; loader `com.abc.nexus`; it reinstalls from the `/oem/` partition, so only clean firmware removes it. Capabilities include silent installs, disabling Play Protect, shell as system, residential-proxy modules and ad fraud. Named model: MECOOL KM9PRO Max.[4]

Published domains: `anyevonline[.]com`, `mqtt.szbboys[.]com`, `file.anyevonline[.]com`, `mqtt.anyevonline[.]com`, `videostrong[.]cn`. **MAG212:** unmanaged boxes in lobbies, staff rooms and clinics become proxy exits and footholds. Block the domains, then isolate or remove the devices.

READ-ONLY · adb · developer mode on the device

```
adb shell pm list packages | grep -iE "oemservice|abc.nexus"
```

Package names per BleepingComputer. A hit means reflash or retire. Not executed by MAG212.[75]

RANSOMWARE THREE CASES

Backups as a credential vault, NAS on the internet

3AM at a UK school estate

Confirmed (Bitdefender command logs): on Sep 10 a modified `Veeam-Get-Creds.ps1` queried the `VeeamBackup` database on `VEEAMSQL2016` and decrypted stored credentials with DPAPI; a Veeam REST probe used port 9392 with Basic auth. Backdoor Domain Admins `library` and `svc_bkpmon`; scheduled tasks `VEEAMPROBE` and `WindowsTempDiag` as SYSTEM; on Sep 18 `dnscmd` and `netdom` built conditional forwarders and two-way trusts between separate school domains; the encryptor ran Sep 19. Bitdefender suspects an automated retry loop from 41–49 s spacing but can't name a model or rule out a human.[15]

Caveat we missed in our Nov 4 daily: Bitdefender's own counts disagree (about 37 encrypted, 47 listed, timing implying ~120; three vs four domains). Initial access is unknown.

READ-ONLY · PowerShell · RSAT / DC Security log read

```
Get-ADTrust -Filter * | Select Name,Direction,TrustType,WhenCreated
Get-ADGroupMember 'Domain Admins' -Recursive | Select Name,SamAccountName
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4706,4720,4728,4698} -MaxEvents 200
Get-ScheduledTask -TaskName VEEAMPROBE,WindowsTempDiag -ErrorAction SilentlyContinue
```

Event IDs are standard Windows auditing (new trust, user created, group add, task created), MAG212's mapping, not Bitdefender's. Not executed by MAG212. [76]

Synology C3RB3R: two advisories, one rule

Reported (BleepingComputer, Nov 2): Synology says attackers exploit "a vulnerability patched in December 2024" on outdated DSM and pointed to SA-24:20 (CVE-2024-10441, CVSS 9.8). A researcher ("360") instead ties its cases to SA-26:13 (CVE-2026-13684, CVE-2026-13639, both 9.8, Sep 18), which itself mentions no exploitation. Files get `.L0CK3D`; the note is `read-me3.txt`. Shadowserver tracks 380,000+ exposed Synology NAS. [77][78][79]

MAG212: a box on 7.2.2-72806-1 is fixed for SA-24:20 but still exposed to SA-26:13 below 72806-9. Run the newest DSM (7.4-90075 / 7.3.2-86009-4 / 7.2.2-72806-9 / 7.2.1-69057-12 minimums), take DSM off the internet (TCP 5000/5001), and keep immutable snapshots.

Queens Public Library

Reported (The Record, NY1): ransomware confirmed Nov 4; website, app, self check-out, on-site computers and Wi-Fi down across 66 branches, which stayed open; NYPD and FBI involved; late fines waived; no group had claimed it and data impact was undetermined as of Nov 5 evening. No technical detail has been published.[25][80]

05 THREAT ACTORS & MOBILE

APT29 (SEKOIA ATTRIBUTION) STATE-BACKED

APT29's watering holes: three exploit kits for stale phones

Sekoia attributes, with moderate-to-high confidence, a campaign that fingerprints visitors and serves known exploit chains only to vulnerable iPhones and Android phones. No zero-days. No persistence. Fully updated devices were not affected.

PUBLISHED	DELIVERY	KEV LINK	VICTIMS
Sekoia · Nov 4	**Hacked sites · AiTM proxies · Plerdy tracker**	**CVE-2024-27834 = Class A stage 2**	**US, UA, CZ, BG, UK, AU**

Class	Target	Chain (CVE per Sekoia)	Takes
A	iOS 16.7 (works 16.0–17.4)	RCE CVE-2025-43529 → PAC bypass **CVE-2024-27834**	Browser cookies → `ad.starx-net[.]com:8881/telemetry/v12`
B "DarkSword"	iOS 18.5	CVE-2025-43529 + CVE-2026-20700 → sandbox CVE-2025-14174, -43510 → kernel CVE-2025-43520	Messages, mail, WhatsApp/Telegram, Keychain, Wi-Fi keys, photos, location
C	Chrome 139–145 on Android (not 143)	Renderer CVE-2026-3910 → Adreno driver CVE-2025-27038	"AndroSnitch": Chrome cookies, history, logins, Wi-Fi

Class B is nearly identical to a leaked commercial iOS kit uploaded to VirusTotal in September. Fixed iOS versions for the Class B CVEs were not re-verified this week; enforce the current release.[23]

How targeting works

An injected script loads "UltimateFingerprinter" (61 collectors, 394 fields: canvas, audio, WebGL, fonts, WebRTC, sensors), POSTs to a nonce endpoint, and only then gets exploit JavaScript. Implausible screen sizes or `navigator.maxTouchPoints = 0` return an empty 200, which defeats desktop sandboxes. Delivery: compromised sites (a Ukrainian gas company, a US chemical trade association, a European political party, a Bulgarian military-related site); reverse proxies impersonating america250.org and Raffles London at The OWO; and Ukraine's Plerdy analytics tracker, Aug 27–Sep 3.[23]

Defend

- MDM: block corporate access below the current iOS; flag 16.x, 17.0–17.4 and 18.5 or older; Android Chrome ≥ 157.
- Class B victims: full-device compromise; rotate mailbox, messaging, Keychain-stored credentials, Wi-Fi keys.
- Your own sites: inventory third-party scripts; SRI and CSP so you're nobody's watering hole.

Role (Sekoia)	Indicator (defanged)
Exfiltration / staging	`ad.starx-net[.]com (195.58.140[.]105) · /api/<nonce>/v1|v2|v3 · port 8881`
Delivery	`static.flux-telemetry[.]com · edge-ord.clouds-stacks[.]com · adsprism-stat[.]com`
AiTM look-alikes	`theowo[.]club (188.190.17[.]232) · america250[.]holiday (192.121.46[.]25)`
Other domains	`ads-it-assets[.]com · cdn.adv-static[.]com · wpvortex-mod[.]com · assets-int[.]com · a.plerdy[.]com (compromised legit)`
AndroSnitch SHA-256	`387a7fb768db1350a9788d9704e7a72abe07152734e0ff026af72b417e36268c`

13 hashes are listed in Sekoia's report; some IOCs are reserved for its customers.[23]

PLATFORM PATCHES · INDIA BFSI CAMPAIGN

Android's no-click RCE, Chrome 157, and Crafty Falcon

Android November bulletin

Confirmed (Google, Nov 2, revised Nov 6): CVE-2026-58868, a critical Framework RCE that needs no user interaction, on Android 14–17. Patch level `2026-11-01` fixes it; `2026-11-05` covers the whole bulletin, including critical kernel, pKVM, Bluetooth and MediaTek modem items. Root cause reported as a heap overflow in `onOutputReceived` of `FrameDecoder.cpp`. Google is not aware of exploitation.[18]

Chrome 157

Reported (secondary summary of Google's post, Nov 3): 157.0.8103.38/.39 with 213 security fixes, 7 critical (Dawn, ANGLE, WebGL, Prerender, Geometry, Core). None flagged exploited. Chrome 157 also lifts Android phones above APT29's Class C range.[43]

READ-ONLY · adb / PowerShell · user

```
adb shell getprop ro.build.version.security_patch           # want 2026-11-01 or later
adb shell dumpsys package com.android.chrome | grep versionName
(Get-Item "C:\Program Files\Google\Chrome\Application\chrome.exe").VersionInfo.ProductVersion
```

Use MDM compliance rules for fleets; these are spot checks. Not executed by MAG212.[75]

CERT-IN CIAD-2026-0058 CRITICAL ADVISORY

Crafty Falcon steals through lenders' own APIs

Confirmed (CERT-In, Nov 4, page updated Nov 7): an AI-assisted actor targets NBFCs, digital lenders, fintechs, payment aggregators and crypto VASPs, re-targeting firms that had remediated, and timing attacks for weekends and holidays. Tools named: the ARTEX family, PentAGI, Cairn and CyberStrikeAI. No public IOCs or CVEs.[13]

Tactics: abuse of AWS Systems Manager and Lambda; pivots from exposed UAT/staging into production via shared credentials; modified client apps calling APIs directly; allow-list bypass through whitelisted third-party "fetcher" IP pools that can be induced to fetch attacker URLs; Rs 1 test transfers before large ones; settlement-API abuse; web shells via fresh PHP/Node.js upload and deserialization flaws; bursts of AI-generated script variants.[13]

CERT-In's controls: default-deny egress (no internet for serverless by default), IMDS protection, non-prod isolation, read-only deploy directories with FIM, request signing with nonce and timestamp, app attestation, mTLS instead of IP allow-lists, holds after micro-transfers, maker-checker on settlement, and monitoring for AI coding agents running with permission checks disabled and LLM API traffic from servers.[13]

READ-ONLY · AWS CLI · cloudtrail:LookupEvents

```
aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=SendCommand \
  --start-time 2026-10-01T00:00:00Z
find /var/www -type f \( -name '*.php' -o -name '*.js' \) -mmin -1440 -ls     # root, web servers
```

Repeat lookup for `UpdateFunctionCode20150331v2` and `CreateAccessKey`. Not executed by MAG212.[81]

FROM OUR NOV 2 TECHNICAL EDITION BACKGROUND RESEARCH

SysGoRAT on Linux, and a help-desk call that ended in AD CS

SysGoRAT (Unit 42, Oct 15)

Confirmed (Unit 42, cluster CL-UNK-1211): government Linux servers, databases and qmail, Oct 2025–Apr 2026. PwnKit (CVE-2021-4034) for root. `auto_prepend_file` rewritten across `/etc/php/` and `/opt/plesk/php/` to load `/usr/lib/php/plesk_sys_driver.php`. The Go RAT installs to `/usr/local/bin/`, writes `/etc/systemd/system/sys-update.service`, adds a 5-minute cron job and an SSH key; GSocket hides in `/dev/shm/.gs-10085/`; SUID helpers `.libsystemd-helper` and `.tourch`. A `.bashrc` sudo alias logs passwords to `Solarwinds.StatusLog.txt` (no SolarWinds compromise). C2 over `wss://…/ws`, default `104.194.158[.]65:443`. Comments in the scripts suggest LLM generation (Unit 42 assessment).[82]

READ-ONLY · Linux · bash · root

```
grep -RHn 'auto_prepend_file' /etc/php /opt/plesk/php 2>/dev/null
systemctl cat sys-update.service 2>/dev/null; ls -la /dev/shm /usr/lib/x86_64-linux-gnu/.l* 2>/dev/null
find / -xdev -perm -4000 -type f -newer /etc/hostname 2>/dev/null
```

A hit means rebuild, not clean. Not executed by MAG212.

Teams “IT support” → Quick Assist → ESC1/ESC8 (Microsoft, Oct 30)

Confirmed (Microsoft): external-tenant Teams calls with support-themed names led users to start Quick Assist; an archive extracted to a `KB`-prefixed folder ran a portable Python, Bun or Java runtime. Case 1 abused an ESC1 template to issue certificates for privileged accounts, then DCSync; an account excluded from automatic containment exfiltrated data with Rclone renamed `SearchApp.exe`. Case 2 used PetitPotam coercion and NTLM relay to AD CS Web Enrollment (ESC8) for a DC certificate and a PKINIT ticket.

Reported (The Hacker News): 3 then 16 users targeted in waves 90 minutes apart.[83]

Microsoft’s fixes: KB5005413; HTTPS with EPA on enrollment endpoints; disable NTLM where possible; remove requester-supplied subject and broad enrollment from templates; remove unneeded Web Enrollment; enable Certification Services auditing. Revoking a certificate does not cancel Kerberos tickets already issued.[83]

CHANGE (first two) / READ-ONLY · CA server · elevated

```
auditpol /set /subcategory:"Certification Services" /success:enable /failure:enable
certutil -setreg CA\AuditFilter 127          # then restart CertSvc
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4886,4887} -MaxEvents 500
certutil -view -restrict "Disposition=20" -out "RequestID,RequesterName,CommonName,CertificateTemplate"
```

4886/4887 (request received/issued) and requester ≠ subject review are MAG212 additions, not in Microsoft’s post. Not executed by MAG212.[84][76]

LOADERS, HEISTS AND PHISHING KITS

NetamLoader, the Binance attribution, and a kit that fakes its takedown

NetamLoader hides in the Windows Update folder (Kaspersky, Oct 29)

Confirmed (Securelist): one victim in Asia, on a government-only custom Windows 10 build; unattributed. A CAB in `C:\Windows\SoftwareDistribution\Download\` uses a legitimate `PatchMyPC-ScriptRunner.exe` whose `.exe.config` triggers AppDomainManager injection, then a BinaryFormatter gadget, AES-layered XAML, an AMSI patch (Scan returns clean) and `COMPlus_ETWEnabled=0`; the final stage runs in `dllhost.exe` via COM. It deletes staged files, CLR usage logs and Prefetch. C2: `openaigpt4v[.]com` (104.18.14[.]219), 5–6 minute polling. No Patch My PC compromise was found; delivery is unknown.[85]

READ-ONLY · Windows · PowerShell · admin

```
Get-ChildItem C:\Windows\SoftwareDistribution\Download -Recurse -Force `
  -Include *.config,*.resx,PatchMyPC-ScriptRunner.exe | Select FullName,Length,LastWriteTime
[Environment]::GetEnvironmentVariable('COMPlus_ETWEnabled','Machine')
```

Not executed by MAG212.

Binance: FBI names TraderTraitor

Reported (Al Jazeera, Nov 1; AAP, Nov 3): the FBI attributed the record $6.3bn theft to North Korea's TraderTraitor, the group blamed for Bybit in 2025, and gave suspected addresses to exchanges (not published). Binance's co-CEO cited a compromised laptop and evidence-deleting malware; Binance says it covered 90% and reopened withdrawals. North Korea called the claim "absurd rhetoric" on Nov 3. No source links NetamLoader to Binance. (Binance was in our Oct 31 weekly; only the attribution is new.)[16]

KELA: the phishing page that pretends it was taken down

Confirmed (KELA, updated Nov 3): 248 live domains imitating 189 US financial institutions (300+ since May). The kit logs the visitor IP: the first visit gets the bank login; a repeat visit from the same IP gets "This account has been suspended," so takedown checkers think it's gone. It blocks devtools and anonymization networks, sits behind Cloudflare, and captures user ID, password and business Company ID. Example domains: `53primaryset[.]com`, `protect-pinnaclefp[.]com`, `authorize-valley[.]com`, `commercial-atfirst[.]com`. A UK home connection is "a lead rather than an identification."[21]

MAG212: brand-protection teams should confirm takedowns from fresh, non-anonymized IPs over several days, and watch new registrations pairing urgency words (secure, protect, authorize, cancel) with bank names.

06 AI, BREACHES & POLICY

AI SECURITY THIS WEEK

AI as target, tool and gatekeeper

ChatGPT Lockdown Mode escaped through a nested iframe

Confirmed (Check Point Research, Nov 5): ChatGPT's HTML-preview iframe carried `allow-popups` and `allow-popups-to-escape-sandbox`. ChatGPT replaced `window.open` only in the preview's own window, so a child iframe's `contentWindow.open("about:blank")` was not blocked and the popup ran unsandboxed. In the Electron "ChatGPT Classic" app, chat exfiltration needed no click. OpenAI removed both tokens on Sept 18; Check Point confirmed the fix. No CVE; nothing for customers to patch.[29]

Lesson for builders: sandbox flags compose across nested frames. Patching an API in one window does not patch it in a frame that window creates.

AI agents and 1,169 Linux root exploits

Reported (SecurityWeek, Nov 5; OpenAI's own post was unreachable): 2,308 bugs flagged, 1,724 confirmed, 1,169 working local privilege-escalation exploits and 291 info-leak proofs, with 948 patches written (not merged). About $1.2M in API spend, roughly $1,279 per exploit, using an unreleased cyber model; a July run found 166. No CVEs or kernel version boundaries were published. **MAG212:** assume kernel LPE supply will rise; prioritize kernel patch cadence and limit local footholds.[86]

GPT-6 Cyber: access behind hardware keys

Confirmed (OpenAI system card, Nov 5): "Access to GPT-6 Cyber is restricted through Daybreak Red": invitation, identity and liveness checks, legal attestation and a physical FIDO2 key for individuals; SSO, MFA, managed devices and least privilege for organizations; IP allowlisting by default for API access. OpenAI rates it "Critical" for cybersecurity. Benchmark gains are not evidence of real-world attacks.[30]

Policy and law enforcement

Japan (Nov 6): the Ministerial Meeting on Cybersecurity, chaired by PM Takaichi, adopted an emergency package: an IPA "Top Gun" team, AI vulnerability-check support for municipalities, a police rapid-forensics unit, recovery support for small businesses, severity-scaled response teams, and a 24/365 monitoring pilot. It cites unpatched flaws, misconfiguration, weak development security and contractor gaps as weaknesses AI makes faster to exploit. No budget published.[34]

US DOJ (Nov 5): three men charged over about $129M taken by using AI to fake the voices and images of real CEOs and lawyers; named victims include hospitals in Missouri and California, a Rhode Island bank and a UK tech firm. Allegations, not convictions.[31]

AI in attacks (assessments): CERT-In names AI tooling in Crafty Falcon; WorkOS links its breach to ARTEX; Bitdefender suspects an automated loop in 3AM; Unit 42 sees LLM-style comments in SysGoRAT scripts; Volexity assesses possible LLM use in the Ivanti exploit (medium confidence).[13][14][15][82][5]

BREACH LEDGER · NOV 1–7

Who lost what this week

Organization	Entry	Exposed (as stated)	Action for customers
Chainalysis	Not disclosed ("on-path"; "agentic")	Names, usernames, password hashes, live tokens: all users. KYT, Reactor offline.[11]	Reset, rotate API keys after IP allowlisting, review API logs.
cPGuard / OPSSHIELD	Billing portal, stolen storage key	Root secrets on ~2,950 servers; ~7,900 billing accounts.[1]	Full root-credential rotation; see page 16.
Northflank	Patched "CVE-2026-98432"	All env vars assumed decrypted from Oct 30.[10]	Revoke at issuer, then rotate.
Chainstack	Third-party component	Names, emails, password hashes; node credentials.[20]	Passwords, node credentials, API keys.
WorkOS	Internal sales app	CRM and support summaries.[68]	Watch for tailored phishing.
DreamHost	Flaw in third-party file-manager software	FTP/SFTP credentials (Aug–Oct 23), some webmail credentials and mailbox content; "well under ~10%" of accounts. TechCrunch, citing a CA AG filing, reports session tokens too.[87]	Rotate FTP/SFTP and mail passwords; check site files.
DigiCert	Feb 2025 migration exposed a business system	Business contacts; a "small minority" with ID documents. Access Jun 27–Jul 2, 2026. Certificates unaffected; no count.[88]	Verify any "DigiCert" contact through the portal.
Norad	27 compromised accounts	Up to 20,614 grants-portal users, incl. applicants in conflict zones.[89]	Applicants: expect targeted contact.
Polymarket	Third-party script via vendor DNS	~$2.6M drained from 33 wallets' positions; $3.9M refunded.[9]	None required; refunds automatic.
Queens Library	Ransomware	Services across 66 branches; data impact undetermined.[25]	Watch for notification.

Reading the ledger

MAG212 analysis: six of ten entries exposed credentials or tokens that stay valid until someone rotates them. The breach date matters less than the rotation date. For each vendor you use, record when you rotated, which keys and where they were stored.

The phishing that follows

Real customer lists (DigiCert, WorkOS, Norad, Chainalysis) produce messages that quote real names, account details and support history. Accurate details do not authenticate a sender; use the vendor portal or a known contact.

Also patched quietly

Microsoft Paint CVE-2026-83844 (CVSS 8.1 RCE) is fixed only through the Microsoft Store (11.2609.401.0 per MSRC); Store apps update per user, so check each profile.[45]

READ-ONLY · Windows · PowerShell 5.1+ · admin for -AllUsers

```
Get-AppxPackage -AllUsers -Name Microsoft.Paint | Select-Object Name, Version, PackageUserInformation
```

Compare against MSRC's fixed build. Not executed by MAG212.

07 DETECTION ENGINEERING

MITRE ATT&CK · TECHNIQUES SEEN THIS WEEK

The week mapped to ATT&CK

Where a researcher published the mapping we say so; everything else is MAG212's mapping from the documented behavior. Use it to check which of your detections would have fired.

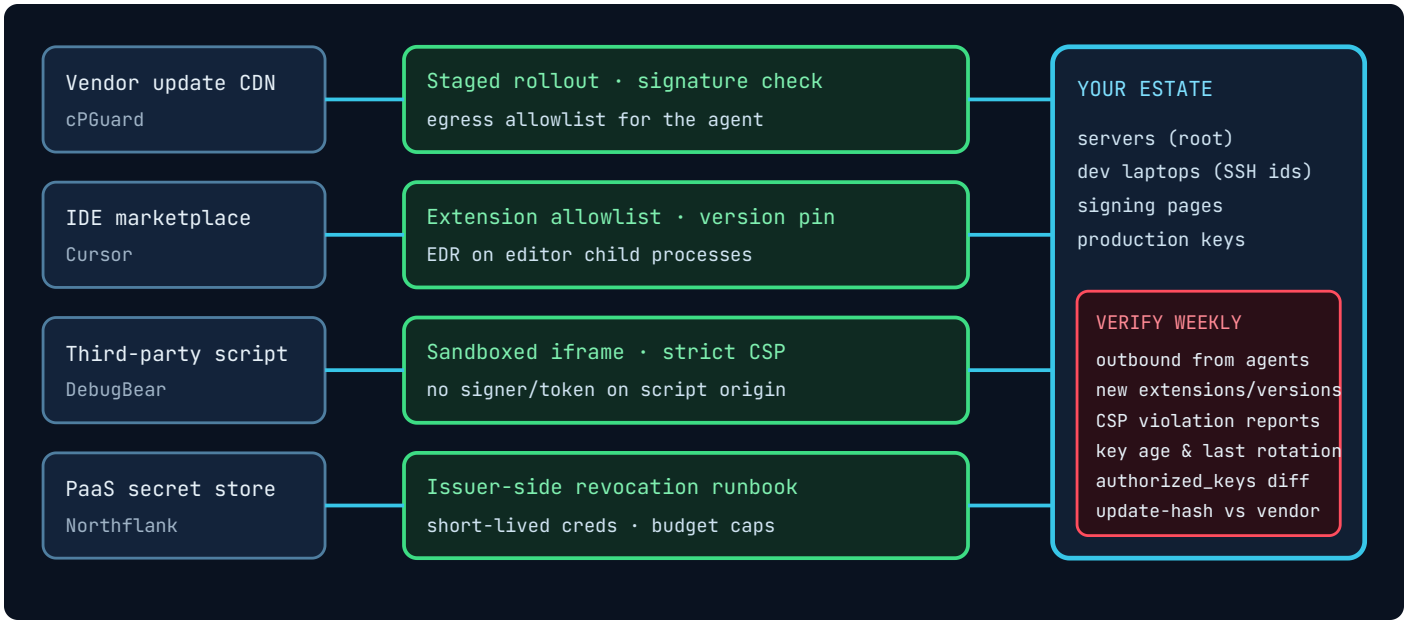
Tactic	Technique	Seen in	Your telemetry
Initial access	T1190 Exploit public-facing application	Ivanti, SonicWall, PAN-OS, Barracuda, Zyxel, OFBiz, PHP2Shell, GitLab, Node-RED	WAF, VPN, appliance logs
	T1195.002 Compromise software supply chain	cPGuard update, Cursor extension, Plerdy tracker (APT29)	EDR, package inventory
	T1189 Drive-by compromise	APT29 watering holes; DebugBear script	Proxy, DNS, MDM
	T1566.003/.004 Phishing via service / voice *(Microsoft)*	Teams "IT support" → Quick Assist	Teams external-access logs
	T1078 Valid accounts	SonicWall alternate auth; Norad (27 accounts)	IdP vs VPN correlation
Execution	T1059.004 Unix shell · T1059.007 JavaScript	cPGuard script; Node-RED exec node; Cursor loader	Process creation (Linux/macOS)
Persistence	T1543.002 Systemd service · T1053.003 Cron	SysGoRAT `sys-update.service`; cPGuard cron; Cursor @reboot	File events on unit/cron paths
	T1098.004 SSH authorized keys	Cursor `svc-telemetry`; SysGoRAT	FIM on authorized_keys
	T1505.003 Web shell	PHP2Shell chain; SysGoRAT prepend; Crafty Falcon	Web-root FIM, PHP-FPM children
	T1053.005 Scheduled task	Cursor "SysMon"; 3AM VEEAMPROBE	Event 4698
Priv. escalation	T1068 Exploitation for privilege escalation	Ivanti dsinvoked; kernel CVE-2026-46300; APT29 kernel stage	Memory forensics
Defense evasion	T1562.001 Impair defenses (AMSI) · T1562.006 (ETW)	NetamLoader	AMSI/ETW tamper alerts
	T1070 Indicator removal *(T1070.006 per Unit 42)*	Ivanti log truncation; SysGoRAT; NetamLoader	Off-box log forwarding
	T1574.014 AppDomainManager	NetamLoader	.config files beside signed EXEs
Credential access	T1649 Steal or forge certificates *(Microsoft)*	AD CS ESC1/ESC8	CA events 4886/4887
	T1555 / T1552.001 Credentials in stores / files	3AM Veeam DB; cPGuard `.my.cnf`; Rails secret_key_base	DB audit, FIM
	T1539 Steal web session cookie	APT29 Class A/C; Chainalysis tokens	Token anomalies at IdP/API
Lateral / impact	T1021.001 RDP · T1484.002 Domain trust modification	PAN-OS ransomware; 3AM rogue trusts	Event 4706, RDP logons
	T1486 Data encrypted · T1657 Financial theft	3AM, C3RB3R, Queens; Polymarket, Crafty Falcon, Binance	Backup alerts, payment controls
C2 / exfil	T1572 Protocol tunneling · T1071.001 Web	Cursor reverse SSH; SysGoRAT wss; NetamLoader HTTPS	Egress, SSH to internet

Microsoft's AD CS post lists T1566.003, T1566.004, T1219, T1649 and others; Unit 42 maps T1070.006 for SysGoRAT. All other mappings are MAG212's.[83][82]

DEFENSIVE ARCHITECTURE · MAG212 RECOMMENDED PATTERN

Putting controls on the channels you trust

Every major intrusion this week rode a trusted channel. This is how to put a checkpoint on each one, and how to prove the checkpoint works.



MAG212 CYBER reference pattern; illustrative architecture, not a vendor design.

1 · Vendor updates

Give security agents and panels an egress allowlist (vendor update host only) and alert on anything else; cPGuard's script exfiltrated to the vendor's own licensing server, so also baseline the *volume* of agent uploads. Stage updates to a canary ring first. Where vendors publish hashes or signatures, verify them in your pipeline.[1]

2 · IDE extensions

Maintain an allowlist of extension IDs and versions; disable auto-update for extensions on admin and release-engineering machines; alert when an editor process spawns `ssh`, `autossh`, `schtasks` or `launchctl`. Treat developer SSH identities as production credentials.[8]

3 · Third-party scripts

Never load analytics or RUM on the same origin as a wallet signer, payment form or session-bearing API; isolate them in a sandboxed iframe or a separate origin. Use CSP with `report-to`; SRI where the vendor offers versioned files. Monitor your vendors' DNS for changes.[9]

4 · Platform-held secrets

Prefer short-lived, workload-identity credentials over static env vars; keep a written runbook that revokes at the issuer (AI provider, cloud, payment) in minutes; set provider budget limits so a stolen AI key can't run up unbounded bills. Rehearse it.[10]

5 · Identity paths at the edge

Every authentication method a VPN accepts is a path an attacker can try. Enumerate them, disable the ones you don't need, and correlate VPN sessions with IdP/MFA events daily (SonicWall).[2]

SIGMA RULES OF THE WEEK · ENDPOINT

Sigma rules you can adapt today (1/2)

Written by MAG212 from the published indicators and behaviors on the pages cited. Not tested against production telemetry: validate field names for your backend (e.g., with sigma-cli) and tune before alerting.

SIGMA · process_creation · Linux/macOS/Windows

```
title: Reverse SSH tunnel exposing local sshd
description: Cursor trojanized extension IOC (Oct 29)
status: experimental
logsource:
  category: process_creation
detection:
  sel_ssh:
    CommandLine|contains|all:
      - ' -R '
      - ':0:localhost:22'
  sel_autossh:
    CommandLine|contains: 'autossh -M 0'
  condition: 1 of sel_*
falsepositives:
  - Admins publishing sshd via reverse tunnels
level: high
```

SIGMA · process_creation · Windows

```
title: Scheduled task named SysMon created
description: Cursor extension persistence (Windows)
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: '\schtasks.exe'
    CommandLine|contains|all:
      - '/create'
      - '/tn SysMon'
  condition: selection
level: high
```

SIGMA · file_event · macOS

```
title: Fake Apple LaunchAgent com.apple.sysmond
logsource:
  product: macos
  category: file_event
detection:
  selection:
    TargetFilename|endswith:
      -
'/Library/LaunchAgents/com.apple.sysmond.plist'
      - '/.config/.smt'
      - '/.config/.smtk'
  condition: selection
level: high
```

SIGMA · file_event · Windows

```
title: Config or resx staged in Windows Update
download
description: NetamLoader AppDomainManager staging
logsource:
  product: windows
  category: file_event
detection:
  selection:
    TargetFilename|contains:
'\SoftwareDistribution\Download\'
    TargetFilename|endswith:
      - '.exe.config'
      - '.resx'
      - '\PatchMyPC-ScriptRunner.exe'
  condition: selection
level: medium
```

SIGMA · process_creation · Windows

```
title: SearchApp.exe outside SystemApps (renamed
tool)
description: Rclone renamed SearchApp.exe (Microsoft
AD CS case)
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: '\SearchApp.exe'
  filter_legit:
    Image|startswith: 'C:\Windows\SystemApps\'
  condition: selection and not filter_legit
level: high
```

Sources for behaviors: Cursor notice; Kaspersky Securelist; Microsoft Security blog.[8][85][83]

SIGMA RULES OF THE WEEK · LINUX, AD AND WEB

Sigma rules you can adapt today (2/2)

SIGMA · file_event · Linux

```
title: cPGuard compromise and SysGoRAT artifacts
logsource:
  product: linux
  category: file_event
detection:
  sel_cpguard:
    TargetFilename|startswith:
      - '/var/tmp/.cpg91511'
      - '/var/tmp/.i93677'
  sel_cron:
    TargetFilename: '/etc/cron.d/i93677'
  sel_sysgorat:
    TargetFilename: '/etc/systemd/system/sys-
update.service'
  condition: 1 of sel_*
level: critical
```

SIGMA · process_creation · Linux

```
title: Node-RED spawning downloader into tmpfs
description: IoT2050 CVE-2026-58115 exploitation
pattern
logsource:
  product: linux
  category: process_creation
detection:
  selection:
    ParentImage|endswith: '/node'
    Image|endswith:
      - '/wget'
      - '/curl'
      - '/sh'
    CommandLine|contains:
      - '/dev/shm/'
      - '/tmp/.'
  condition: selection
level: high
```

SIGMA · process_creation · Windows DC

```
title: New domain trust or DNS forwarder via CLI
description: 3AM ransomware rogue trusts
(Bitdefender)
logsource:
  product: windows
  category: process_creation
detection:
  sel_netdom:
    Image|endswith: '\netdom.exe'
    CommandLine|contains|all: ['trust', '/add']
  sel_dnscmd:
    Image|endswith: '\dnscmd.exe'
    CommandLine|contains|all: ['/zoneadd',
'/dsforwarder']
  condition: 1 of sel_*
level: high
# pair with Security EventID 4706 (trust created)
```

SIGMA · webserver · any

```
title: PHP requested under WordPress upgrade staging
description: CVE-2026-119977 upgrade-window probing
logsource:
  category: webserver
detection:
  selection:
    cs-uri-stem|contains: '/wp-content/upgrade/'
    cs-uri-stem|endswith: '.php'
  plugin:
    cs-uri-stem|contains: '/cryptopayment-
gateway/vendor/cryptd/'
  condition: selection or plugin
level: high
```

Before you deploy. Run every rule through `sigma check` and a 30-day backtest. Expected noise: Node-RED rule on boxes that legitimately use exec nodes; web rule during your own maintenance windows.

Behaviors from OPSSHIELD, Unit 42, VulnCheck via The Hacker News, Bitdefender, Wordfence CNA/WPScan.[1][82][74][15][37][38]

CONSOLIDATED INDICATORS · EXACTLY AS PUBLISHED, DEFANGED

Hunt pack: network indicators of the week

Feed these to DNS, proxy, firewall and EDR searches for Oct 1 onward. An indicator hit is a lead, not proof; infrastructure is often shared or recycled.

Campaign	Domains / URLs	IPs	Source
Ivanti UTA0576	header X-DSCGI-PATH · /dana-na/auth/url_default/welcome.cgi bursts	108.165.147[.]64	Volexity[5]
PAN-OS 0257	host IDs aa:bb:cc:dd:ee:ff, 00:11:22:33:44:55 · names WINDOWS-LAPTOP-001, DESKTOP-GP01, GP-CLIENT	23.128.228[.]6 · 104.207.144[.]154 · 146.19.216[.]119/.120/.125 · 179.43.172[.]213 · 185.195.232[.]139 · 198.12.106[.]60 · 202.144.192[.]47	Unit 42[48]
cPGuard	/i90248_probe.txt · /i90573_probe.txt · /i90573_sh.php · /i90573_x.php · *_rx.php · UA cPGuard/5.88.11	94.183.188.91	OPSSHIELD[1]
Cursor extension	POST :8099/beacon · reverse ssh user "tunnel"	134[.]209[.]82[.]225	Cursor[8]
DebugBear drainer	cdn.debugbear[.]com/C7xcKKrjUnXK.js · data.debugbear.com · wallet 0x3F99139F1C5854bb628c2e576Aaf638e99dFfc18	—	BleepingComputer[67]
WorkOS / ARTEX	User agents artex-enrich/1.0 · norma/0.4	—	BleepingComputer[14]
Node-RED IoT2050	wget.sh · .sys_update · /dev/shm/.b · /tmp/.kworker	85.215.73[.]250 · 45.194.90[.]57:38472	VulnCheck via THN[74]
XCPE	anyevonline[.]com · file./mqtt.anyevonline[.]com · mqtt.szbboys[.]com · videostrong[.]cn	—	BleepingComputer[4]
APT29 mobile	ad.starx-net[.]com · static.flux-telemetry[.]com · edge-ord.clouds-stacks[.]com · adsprism-stat[.]com · theowo[.]club · america250[.]holiday · ads-it-assets[.]com · cdn.adv-static[.]com · wpvortex-mod[.]com · assets-int[.]com	195.58.140[.]105 · 188.190.17[.]232 · 192.121.46[.]25 · 109.104.106[.]107 · 95.133.231[.]28	Sekoia[23]
SysGoRAT	magento[.]ink · solidmonpe[.]com · wibu-bau-bawang[.]online · beraskencur[.]site · wss://…/ws	104.194.158[.]65 (+16 in report)	Unit 42[82]
NetamLoader	openaigpt4v[.]com/model_v4/	104.18.14[.]219 (Cloudflare)	Securelist[85]
KELA bank kit	53primaryset[.]com · protect-pinnaclefp[.]com · authorize-valley[.]com · commercial-atfirst[.]com	—	KELA[21]
Zyxel Kapibala	*.981666.xyz · accounts kapibala/kapibala2 · outbound TFTP from switches	74.48.66.73 · 104.225.153.141 · 172.245.247.21	GreyNoise via MAG212[51]

READ-ONLY · Linux · bash · proxy/DNS log read access

```
grep -E -i 'starx-net\.com|flux-telemetry\.com|clouds-
stacks\.com|anyevonline\.com|szbboys\.com|openaigpt4v\.com|debugbear\.com|981666\.xyz' \
  /var/log/squid/access.log*      # adjust path / SIEM
```

Cloudflare and shared-hosting IPs (e.g., 104.18.14[.]219) will produce false positives; prefer domain matches there. Not executed by MAG212.

HOST CHECKS BY PLATFORM · ALL READ-ONLY UNLESS MARKED

Hunt pack: one sweep per platform

READ-ONLY · Linux servers · bash · root

```
# cPGuard, SysGoRAT, PHP webshell hooks, Node-RED droppers, Cursor (Linux)
ls -la /etc/cron.d/i93677 /var/tmp/.cpg91511* /var/tmp/.i93677 /dev/shm/.b /tmp/.kworker /tmp/.stk_*
2>/dev/null
grep -RHn 'auto_prepend_file' /etc/php /opt/plesk/php 2>/dev/null
systemctl list-timers --all; systemctl cat sys-update.service 2>/dev/null; ls -la /etc/cron.d/
find / -xdev -perm -4000 -type f -newer /etc/hostname 2>/dev/null
for f in /root/.ssh/authorized_keys /home/*/.ssh/authorized_keys; do ssh-keygen -lf "$f" 2>/dev/null;
done
php -v; awk -F: '$2=="*"{print $1}' /etc/shadow
```

Compare SSH key fingerprints against your inventory and the Cursor fingerprints on page 17. Not executed by MAG212.

READ-ONLY · Windows · PowerShell · admin / domain read

```
Get-ADTrust -Filter * | Select Name,Direction,WhenCreated                    # 3AM rogue trusts
Get-ADGroupMember 'Domain Admins' -Recursive | Select SamAccountName
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4706,4720,4728,4698,4886,4887} -MaxEvents 500
Get-ScheduledTask -TaskName SysMon,VEEAMPROBE,WindowsTempDiag -ErrorAction SilentlyContinue
Get-ChildItem C:\Windows\SoftwareDistribution\Download -Recurse -Force -Include *.config,*.resx
Select-String -Path $HOME\.ssh\authorized_keys,C:\ProgramData\ssh\administrators_authorized_keys -
Pattern svc-telemetry
Get-AppxPackage -AllUsers -Name Microsoft.Paint | Select Name,Version
```

4886/4887 require Certification Services auditing on the CA. Not executed by MAG212.

READ-ONLY · macOS · zsh/bash · affected user

```
cursor --list-extensions --show-versions | grep -i claude-code
ls -la ~/Library/LaunchAgents/com.apple.sysmond.plist ~/.config/.smt ~/.config/.smtk; launchctl list |
grep sysmond
ssh-keygen -lf ~/.ssh/authorized_keys
```

Not executed by MAG212.

READ-ONLY · Web logs · nginx/Apache · root

```
sudo zgrep -hE '/wp-content/upgrade/[^" ]*\.php|cryptopayment-
gateway/vendor/cryptd/|/sfa/control/editPortalPageColumnWidth|_LAST_VIEW_NAME_|/cgi-
mod/index\.cgi|/jsonapi/commerce_order' \
  /var/log/{nginx,apache2}/access.log* 2>/dev/null | head -200
```

One pass for WordPress, the dead payment plugin, OFBiz, Barracuda and Drupal Commerce markers. Hits need correlation with responses and timing. Not executed by MAG212.

READ-ONLY · Edge / appliances · from outside your network, authorized

```
nmap -Pn -p 443,4433,4443,3879,8443,1880,5000,5001 <your-public-ranges>
```

SSL-VPN (443/4433), GlobalProtect on management (4443/3879), LXD (8443), Node-RED (1880), Synology DSM (5000/5001). Anything answering that shouldn't is this week's top finding. Not executed by MAG212.

ACTION DESK · BY ROLE

What each team should finish before next Saturday

Network & security engineers

- Ivanti to 25.1.1.3 / 22.8R2.6 after memory capture; rotate bind account, LAPS, BitLocker.
- SonicWall to 8.2.3-8015 / newest 7.3.4; prune auth methods; MFA-gap hunt.
- GlobalProtect: patch all portals and gateways together; dedicated override cert.
- Zyxel GS1900 to Patch 3; Barracuda ESG patch confirmed in UI.
- External port sweep (page 34) and a ticket for every unexpected listener.

Platform & DevOps

- cPGuard: full root-secret rotation, including hosts that trust its keys.
- PaaS secrets: revoke at issuer, then rotate; set provider budget limits.
- PHP 8.x fixed builds, restart workers, patch kernel; GitLab Oct 29 builds.
- Rails 8.1.4.1 / 8.0.5.2 + secret rotation; OFBiz 24.09.08; LXD snaps.
- Agent folders in .gitignore, gitleaks rule in CI.

MSPs

- Per-tenant list of Ivanti, SonicWall, PAN-OS, Barracuda, Zyxel and Synology assets with running versions.
- Check every managed Linux server for cPGuard and the IOC paths.
- Synology: newest DSM, no internet-facing DSM, immutable snapshots.
- Backup servers: alert on Veeam DB credential reads and new Domain Admins.

School & public-sector IT

- Audit AD trusts and conditional forwarders (3AM case).
- Isolate backup servers; confirm offline/immutable copies restore.
- Inventory cafeteria and lab refrigeration, TV boxes and signage players.
- Practice a "library down" day: manual checkout, offline procedures.

Business owners & finance

- Two-person rule and call-back for payments (deepfake case).
- Rotate Chainalysis, DreamHost and other vendor credentials named this week.
- Ask suppliers: who can change our systems remotely, and how would we know?

Close the ticket only with evidence: running version on every node, an exposure test from the right network, a configuration diff, a rotation record (what, when, where stored) and a service smoke test. A patch closes the door; it doesn't tell you who already came in.

TWO-MINUTE LESSON · FOR EVERY EMPLOYEE

"IT support" on Teams, the CEO on video, your bank "suspended"

Three tricks from this week

The help-desk call. A Teams message from "IT Support" asks you to start Quick Assist. Microsoft documented this leading to domain takeover. Your IT team will not cold-call you through an external Teams tenant.[83]

The executive on video. Prosecutors say AI-faked voices and faces of CEOs and lawyers pulled about $129M from hospitals, a bank and companies. Urgency plus secrecy plus authority is the pattern.[31]

The page that says it's gone. A phishing kit shows investigators "account suspended" while still harvesting logins from new visitors. If you entered details on a suspicious page, report it even if it now looks dead.[21]

Do this every time

- Verify requests through a channel you already have, not one supplied in the message.
- Never start remote-access tools for an unsolicited caller.
- Two people approve payments and bank-detail changes.
- Update phones and browsers the day updates arrive.

For leaders

This week's worst incidents arrived through trusted vendors. Ask each critical supplier three questions: how do you sign and deliver updates, what of ours do you store decrypted, and how fast will you tell us?

Watch list, Nov 8–14. Microsoft Patch Tuesday (Nov 10) · Ivanti CVE-2026-118527 KEV due (Nov 13) · Apple CVE-2024-27834 KEV due (Nov 18) and SonicWall (Nov 20) · whether CISA lists Zyxel CVE-2026-107441, SSHole or Barracuda · Northflank root-cause report · Chainalysis restoration · any weaponization of the Barracuda, OFBiz or LXD write-ups.

MAG212 CYBER: daily and weekly, free

Verified intelligence, CVEs that matter, and commands you can use, every morning and every Saturday. No cost; unsubscribe anytime.

Subscribe free → cyber.mag212.com/subscribe-free

EDITORIAL TRANSPARENCY

How we checked, and what we corrected

Every story was re-checked between Nov 6 and Nov 7 against vendor advisories, CVE and KEV records, government alerts or the original researcher. Where a primary page could not be reached, the story says so.

Corrections to our daily coverage this week

- **PAN-OS (Nov 1):** CVSS is 7.8 (CVSS 4.0, Palo Alto), not 9.1; KEV date is May 29.
- **Ivanti (Nov 1–2):** the Nov 2 deadline applies only to CVE-2026-111357; CVE-2026-118527 is due Nov 13.
- **SonicWall (Nov 7):** the SAML/MFA bypass we called unconfirmed is stated in CISA's KEV entry.
- **3AM (Nov 4):** Bitdefender's machine and domain counts are internally inconsistent; we now say so.
- **Cursor (Nov 1–3):** "up to 5,000 users" is Reuters quoting Cursor, not text in Cursor's notice.
- **Synology (Nov 3–4):** SA-24:20 is dated Nov 2024; the SA-26:13 link is a researcher claim.
- **Barracuda (Nov 5):** fixed build is 9.4.0.029 per watchTowr's diff vs .030 in press; confirm with Barracuda.
- **cPGuard (Nov 4):** two IPs we listed (5.182.208.x) do not appear on the vendor's pages, so this issue omits them. Fixed version: ≥ 5.88.26.

Pages we could not reach

Ivanti advisory (hub.ivanti.com), SonicWall PSIRT detail page, cisa.gov pages (KEV read from CISA's GitHub data), OpenAI's kernel-research post, Apiiro's blog, Wordfence blog, Google GTIG's XCPE post, VulnCheck's blog, Binarly's article body, Chrome Releases (Chrome 157 via secondary summary), Bitdefender's IOC CSV, the php.net advisory. Facts depending on these are attributed to the secondary source used.

What is still unknown

How Cursor's marketplace was accessed; how cPGuard's storage key was obtained; Northflank's root cause; the "specific certificate configuration" in PAN-OS; which Synology CVE C3RB3R uses; fixed iOS versions for every APT29 Class B CVE; whether SSHole reached production systems; any 2026 CVE behind the refrigeration attacks.

> **Visuals and commands.** All diagrams are MAG212 CYBER explanatory graphics; the cover is a conceptual illustration. No screenshots are used. IOCs are reproduced as published and defanged. Commands were checked against official documentation where reachable and are labelled read-only or change; none was executed by MAG212 on affected systems.

EDITORIAL REGISTER · PART 1

Sources

01 OPSSHIELD · Security incident disclosure (Nov 3)

02 CISA · KEV catalog data, version 2026.11.06 (official GitHub mirror)

03 The Hacker News · Claude Code 'don't ask again' file leaks secrets (Nov 7)

04 BleepingComputer · Google disrupts XCPE botnet (Nov 2)

05 Volexity · Chained exploitation of Ivanti Connect Secure zero-days (updated Oct 29)

06 Rapid7 · Additional Ivanti Connect Secure zero-days exploited (Nov 2)

07 watchTowr Labs · Barracuda ESG pre-auth remote root (Nov 5)

08 Cursor · Claude Code extension security notice (updated Oct 30)

09 The Hacker News · Polymarket drain and DebugBear DNS (Nov 1)

10 Northflank · Incident status page (updated Nov 6)

11 Chainalysis · Security incident updates (latest Nov 6)

12 Rails · GHSA-f3w6-w445-fwh9 Active Storage (Nov 4)

13 CERT-In · CIAD-2026-0058 Crafty Falcon (Nov 4, updated Nov 7)

14 BleepingComputer · WorkOS says attacker used ARTEX AI (Nov 3)

15 Bitdefender · 3AM ransomware hybrid AI attack (Nov 3)

16 Al Jazeera · FBI blames North Korea for $6.3bn crypto heist (Nov 1)

17 Trigger.dev · Security incident (Nov 1)

18 Android Security Bulletin · November 2026 (updated Nov 6)

19 BleepingComputer · Over 1,000 GitLab servers vulnerable (Nov 2)

20 Chainstack · Security incident (Nov 3)

21 KELA · Bank phishing campaign with fake takedown (updated Nov 3)

22 Binarly · Zyxel GS1900 RCE CVE-2026-107441 (Nov 3)

23 Sekoia · Poisoned Source: APT29 watering holes (Nov 4)

24 Siemens ProductCERT · SSA-834709 V1.1 (Nov 4)

25 The Record · Queens library ransomware (Nov 5)

26 CISA/FBI/HHS/USDA/DoT · Harden refrigeration and cold-chain monitoring (Nov 5)

27 Alpine Linux · OpenSSH password authentication bypass (Nov 5)

28 CVE record · CVE-2026-83542 OFBiz (updated Nov 6)

29 Check Point Research · ChatGPT Lockdown Mode bypass (Nov 5)

30 OpenAI · GPT-6 Cyber system card (Nov 5)

31 US DOJ SDNY · AI impersonation fraud charges (Nov 5)

32 Picus · When updating WordPress becomes the vulnerability (Nov 5)

33 Previdian · CVE-2026-123158 sensor page (read Nov 7)

34 Government of Japan · Cybersecurity emergency package (Nov 6, Japanese)

35 SonicWall · SonicOS 7.3.4 / 8.2.3 security advisory notice

36 OPSSHIELD · cPGuard update channel compromise advisory

37 CVE record · CVE-2026-119977 (Wordfence CNA)

38 WPScan · CryptoPayment Gateway 1.2.1–1.2.2 unguarded AJAX router

39 CVE record · CVE-2026-109618 PHP (updated Nov 5)

40 CVE record · CVE-2026-97229 GitLab

41 Canonical · Critical vulnerability in LXD and MicroCloud (Oct 28)

42 Apache OFBiz · Security page (24.09.08, 46 CVEs)

43 Chrome Releases · Stable channel update, Chrome 157 (Nov 3; via secondary summary)

44 The Hacker News · Experts demonstrate Barracuda ESG chain (Nov 6)

45 Microsoft MSRC · CVE-2026-83844 Paint

46 SonicWall PSIRT · SNWLID-2026-0019 (GMS, won't fix)

47 SecurityWeek · Cisco, WatchGuard patch; SonicWall won't fix GMS (Nov 5)

48 Unit 42 · Active exploitation of PAN-OS CVE-2026-0257 (updated Oct 26)

49 Palo Alto Networks · CVE-2026-0257 advisory

50 SonicWall · SonicOS 8.2.3-8015 release notes

51 MAG212 · Zyxel GS1900 CVE-2026-107441 (Nov 5; cites Zyxel, Binarly, GreyNoise)

52 Rescana · LXD/MicroCloud CVE-2026-112816

EDITORIAL REGISTER · PART 2 · OUR DAILY ISSUES THIS WEEK

53 OpenSSH portable · auth-passwd.c
54 OpenSSH portable · xcrypt.c (pick_salt)
55 WordPress.org · WordPress 7.1.4 (Oct 28)
56 The Hacker News · Installing the fix for exploited WordPress flaw (Nov 6)
57 WP-CLI · wp core verify-checksums
58 WP-CLI · wp plugin delete
59 Recorded Future · PHP2Shell exploitation
60 GitLab docs · Access token Rake tasks
61 Rails Guides · Security (secret rotation)
62 Drupal · SA-CONTRIB-2026-254 Commerce Core (Oct 28)
63 Rescana · Drupal Commerce CVE-2026-118539 (Centarro details)
64 Drush · pm:security
65 Reuters via The Star · Cursor says up to 5,000 users affected (Oct 30)
66 VS Code docs · Command-line interface
67 BleepingComputer · Polymarket halts trading after drainer script (Oct 29)
68 WorkOS · Oct 30 data security incident bulletin
69 Anthropic · Claude Code settings documentation
70 CERT-FR · CERTFR-2026-ALE-012 refrigeration controllers (Oct 12–16)
71 Cybersecurity Dive · Thousands of refrigeration devices exposed (Oct 15)
72 Euronews · Cyberattack hits French blood banks (Nov 4)
73 Node-RED · Securing Node-RED
74 The Hacker News · Attackers exploit critical Siemens flaw (Nov 3)
75 Android Developers · Android Debug Bridge
76 Microsoft Learn · Get-WinEvent
77 BleepingComputer · Synology warns of C3RB3R attacks (Nov 2)
78 Synology · SA-24:20
79 Synology · SA-26:13 (Sep 18)
80 NY1 · Ransomware disrupts Queens Public Library (Nov 5)
81 AWS CLI · cloudtrail lookup-events
82 Unit 42 · SysGoRAT / CL-UNK-1211 (Oct 15)
83 Microsoft Security · Help-desk impersonation and AD CS abuse (Oct 30)
84 Microsoft Learn · certutil
85 Kaspersky Securelist · NetamLoader (Oct 29)
86 SecurityWeek · AI agents got root via kernel flaws (Nov 5)
87 DreamHost · October security incident (Oct 29)
88 Mozilla Bugzilla 2084460 · DigiCert incident report
89 Help Net Security · Norad grants portal breach (Nov 5)

·· MAG212 · Daily, Nov 1 (Broken Trust)
·· MAG212 · Technical Edition, Nov 2
·· MAG212 · Daily, Nov 3 (The Forgotten Edge)
·· MAG212 · Daily, Nov 4 (When the Update Becomes the Attack)
·· MAG212 · Daily, Nov 5 (The Patch That Didn't Hold)
·· MAG212 · Daily, Nov 6 (The Cold Chain Is Now a Target)
·· MAG212 · Daily, Nov 7 (SonicWall VPN Flaw Now Exploited)

MAG212 CYBER · Weekly Cyber Intelligence · November 1–7, 2026. Written and edited by El Mostafa Ouchen. Research cutoff Nov 7, 2026 (America/Los_Angeles). Summaries and analysis are original; quotations are attributed. Free subscription: cyber.mag212.com/subscribe-free.