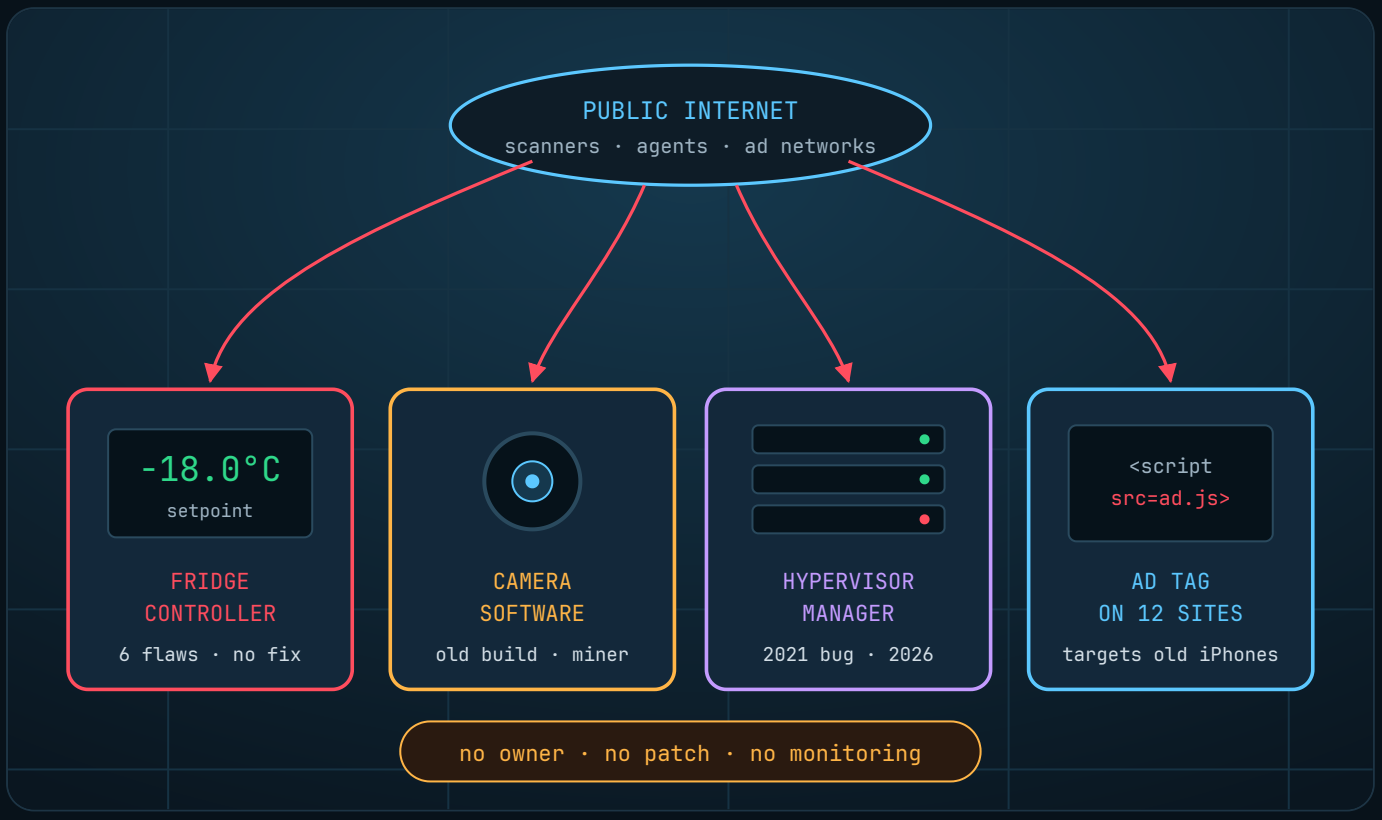
MAG212
CYBER

DAILY

Monday, 16 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 6:00 AM PT



FORGOTTEN INFRASTRUCTURE / NOV 13-16

The boxes nobody patches

A supermarket fridge controller, a camera server, a five-year-old Log4Shell bug on a hypervisor manager, an ad tag on a news site. Today's stories share one cause: equipment that sits on the internet without an owner who patches or watches it.

03 Danfoss fridge controllers: six pre-login flaws, no fix

05 GeoVision camera software turned into a crypto-miner

07 Log4Shell in vCenter led to a code-signing server

09 Amazon: AI agents steal AI keys to pay for more hunting

10 Ads on 12 Dutch sites tried to hack old iPhones

11 KEV due today · Coles · Project Zero goes 'Full 90'

What matters today

This edition covers developments published or updated 13–16 November. Danfoss and ARTEX return from earlier issues because something material changed; we say what.

Cold-chain controllers: worse than patching

Midnight Blue found six pre-login code-execution flaws in Danfoss AK-SM800A firmware up to 5.3.2. There is no fix and no CVE yet. Belgium, Ireland and Germany all say: take the controllers off the internet. [1][2][3]

Unowned software is the entry point

Huntress traced XMRig on 13 organisations to old GeoVision GV-VMS builds. Kaspersky traced a months-long intrusion to an unpatched Log4Shell in vCenter 7.0.3, ending at a code-signing server. [10][12]

AI agents that pay their own way

Amazon's decoys captured ARTEX agents stealing AI provider keys from exposed LiteLLM, Dify and Ollama installs, then spending those keys on the next round of hunting. [15]

Deadlines and disclosure

CISA's KEV due date for UnrealIRCd and Check Point is today. Google Project Zero now publishes bug details 90 days after report, fixed or not, falling to 30 days by 2028. [26][24]

THE THREE PRIORITY ACTIONS

1. **Pull refrigeration and building controllers off the internet.**
   Find every Danfoss, Copeland/Dixell or similar controller reachable from outside, including via a contractor's 4G/5G modem. Put access behind a VPN or private APN; then check setpoints, defrost schedules and users. [1][3]
2. **Hunt for shells spawned by camera and other 'appliance' software.**
   On GeoVision hosts, look for cmd/PowerShell children of GeoStartupAgentService.exe, IFEO hijacks of Defender and the PackageUpdater tasks; upgrade GV-VMS. [10]
3. **Close today's KEV items and lock down AI gateways.**
   Finish UnrealIRCd and Check Point (due today). Require auth on LiteLLM, Dify, Langflow and Ollama, rotate any provider key they stored, and alert on AI spend. [26][15]

CONTENTS

03 Danfoss AK-SM800A: six unpatched pre-auth flaws
04 Danfoss: isolate, check for tampering, verify
05 GeoVision GV-VMS turned into an XMRig loader
06 GeoVision: hunt commands and recovery
07 BO Team: Log4Shell in vCenter to code signing
08 BO Team: what to hunt and how to protect signing
09 ARTEX update: Amazon's agents that steal AI keys
10 Malicious ads on 12 Dutch sites target old iPhones
11 Briefs: KEV due today, Coles, Project Zero, Rspamd
12 Defender's Action Desk
13 Awareness: who owns the box?
14 Sources

UPDATE TO WEEKLY 14 NOV | NO PATCH · NO CVE YET | 3 NATIONAL ADVISORIES | NEW FLAWS: NO EXPLOITATION REPORTED

Danfoss fridge controllers: six ways in, no login, no fix

STATUS **What changed since our Weekly.** Then, the attacks used flaws Danfoss had already fixed. Now, researchers show that even the newest firmware is open to unauthenticated remote code execution, and Strict mode does not fully close it. BSI has no information on exploitation of the six new flaws; endpoints and CVE numbers are withheld and no fix date is published. [1][2][5][30]

WHAT HAPPENED

Carlo Meijer of Dutch consultancy Midnight Blue says he found the flaws in under an hour of manual review, using firmware Danfoss offers for download. Five sit in unauthenticated web request handlers of a program running as root. The sixth is in the gateway that enforces Strict mode. On older firmware 3.3.0 the team ran code as root through one of them. [1][2]

Danfoss lists 5.4.0 (November) as its newest release. Its readme and update guide mention no vulnerability fix, only a stricter password rule. BSI first said 5.4.0 was unaffected, then corrected that to 'cannot rule out'. [1][6]

WHO IS AFFECTED

- Danfoss AK-SM800A system managers, firmware **up to and including 5.3.2**; 5.4.0 not confirmed safe. [1] [2]
- Supermarkets, cold stores, warehouses and pharmacies whose controllers are reachable from the internet, often through a service company's modem. [2]
- Midnight Blue says the same exposure advice applies to Copeland, Dixell and similar controllers. [2]

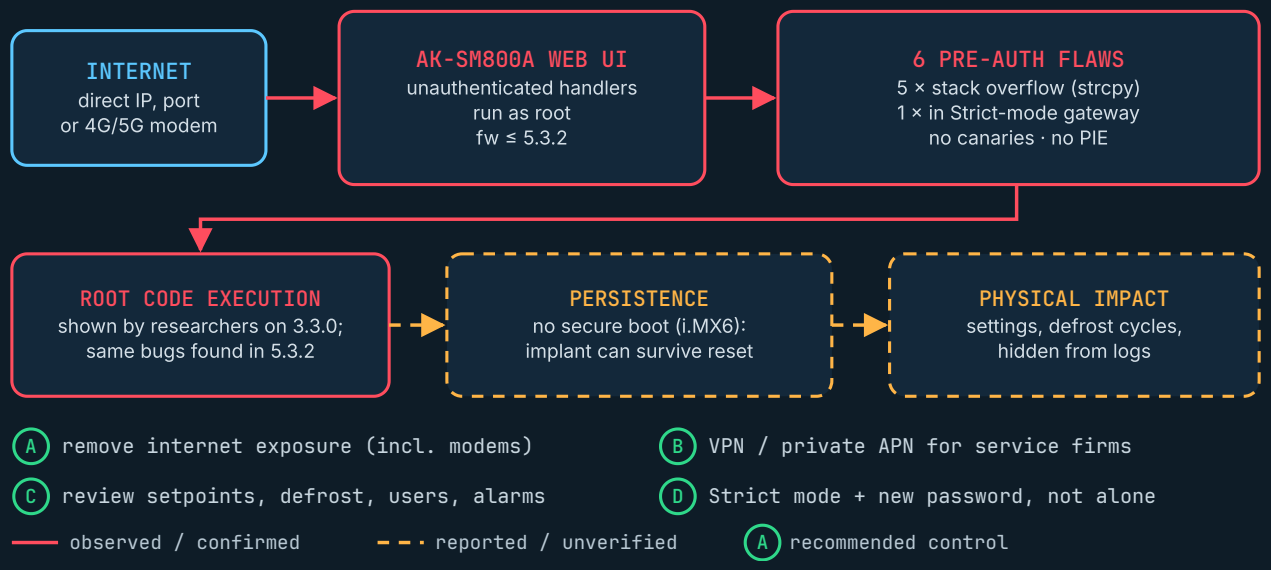


Figure 1 · Attack path described by Midnight Blue. Red = shown by the researchers; amber dashed = capability the researchers describe, not observed in an attack. Diagram: MAG212 CYBER.

DATE	EVENT	STATUS
11 Oct–2 Nov	Attack waves on exposed Danfoss and Copeland controllers, France then Europe	Reported
11 Nov	Midnight Blue discloses six pre-auth RCE flaws (details withheld)	Researcher
12–13 Nov	CCB (Belgium), NCSC (Ireland), BSI (Germany) issue warnings	Government
16 Nov	No Danfoss advisory or fix date; 5.4.0 lists no security fix	Checked by THN

Isolate first, then look for tampering

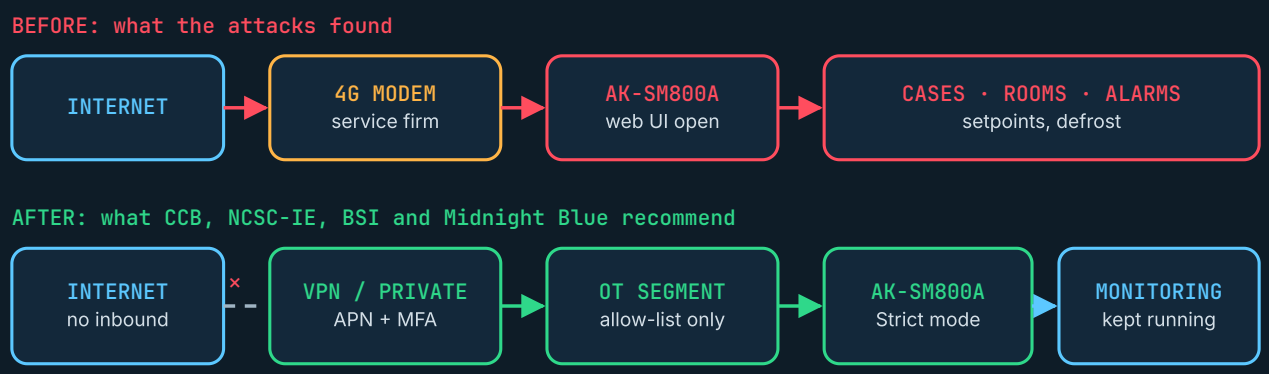


Figure 2 · Defensive architecture based on the CCB, NCSC Ireland and BSI advisories and Midnight Blue's guidance. Conceptual; adapt to your site. Diagram: MAG212 CYBER.

HOW TO INVESTIGATE

1. List every site with an AK-SM800A (and Copeland/Dixell XWEB or similar). Ask each refrigeration service contractor how they connect: fixed IP, port forward, cloud portal or 4G/5G modem. [1][2]
2. From outside, test whether each controller answers on HTTP/HTTPS; check your public ranges in an internet-scan service.
3. Pull alarm history and firewall/modem logs for unknown source IPs.
4. Work through the checklist below with the refrigeration engineer.

LOOK FOR No indicators are published for the six flaws. October's signs were unwanted defrosts and spoiled stock; an attacker could hide from logs, so a clean log is not proof. [1][2]

CONTAIN AND REMEDIATE

1. Remove all direct internet access, modems included; CCB says this applies whatever the patch level. [3]
2. Contractors connect via VPN or private APN; IP allow-lists are a stop-gap. [1][2]
3. Check contract and insurance terms first; keep temperature monitoring alive. [1]
4. Suspected tampering: change all credentials, verify the equipment (BSI). [5]
5. Latest firmware, Strict mode, new password: useful, not sufficient (NCSC-IE). [4]
6. Install Danfoss's fix when its advisory appears. [7]

VERIFY RECOVERY

- Controller address silent from the internet (re-test from outside).
- Contractor access works only via the new path.
- Setpoints, defrost and alarm routing match design.

TAMPERING CHECKLIST · COMPILED BY MAG212 FROM [1]; MENU NAMES VARY BY FIRMWARE

CHECK	WHAT TO COMPARE	RED FLAG
Setpoints	Each case and room against design values	Warm setpoints
Defrost	Frequency, duration, termination temperature	Extra or long defrosts
Alarms	Thresholds, delays, recipients	Muted or redirected
Users	Accounts and roles	Unknown or new admins
Remote access	Port forwards, modems, VPN, notification config	Settings you didn't make

EXPLOITED · 13 ORGANISATIONS | FIX: V17.4.8.58 | CVE USED: NOT IDENTIFIED

The camera server that mined Monero

Attackers broke into an out-of-date build of GeoVision's camera management software and turned it into a launch pad: switch off Defender, plant a loader, mine cryptocurrency.

WHAT HAPPENED

Huntress responded to intrusions at 13 organisations, mostly between 8 and 10 November. Every one began with a service belonging to GeoVision GV-VMS, a Windows video management system. The hosts ran 17.4.8.0, a build compiled in April 2024. [10][11]

GeoVision's April 2026 advisory lists three unauthenticated remote code execution flaws in the WebCam Server function of that version. Huntress has not determined which one was used. Older GeoVision bugs exploited in the wild (CVE-2024-6047, CVE-2024-11120) hit end-of-life embedded devices, not this software. [11]

WHO IS AFFECTED

- GV-VMS installations older than **V17.4.8.58** with the WebCam Server reachable from untrusted networks. [11]
- Organisations where security cameras are run by facilities staff or an installer, outside IT's patch cycle.

HUNTRESS IOCs · 13 NOV · VET BEFORE BLOCKING

Script host	45.32.117[.]34
Loader C2	156.246.94[.]183 · cctv-update[.]top (reg. 7 Nov)
Likely exploit	2.59.133[.]151 (contacted by WebCamServer.exe)
update.exe	f1235751c9e48e5732b7b183dc2bb175a19e4c6401dfd0e96b4cfdd0d8c54b4c
driver	ff5dbdcf6d7ae5d97b6f3ef412df0b977ba4a844c45b30ca78c0eeb2653d69a8
scripts	b673c4d707828abedc767a2be6badef7454492e62c37e30cf3cc5a402fd3647b
Files/tasks	C:\Windows\System32\config\systemprofile\update.exe · ApplyUpdate.exe · PackageUpdater, PackageUpdater_Startup

Source: Huntress [10]. Single-vendor indicators; infrastructure may be reassigned.

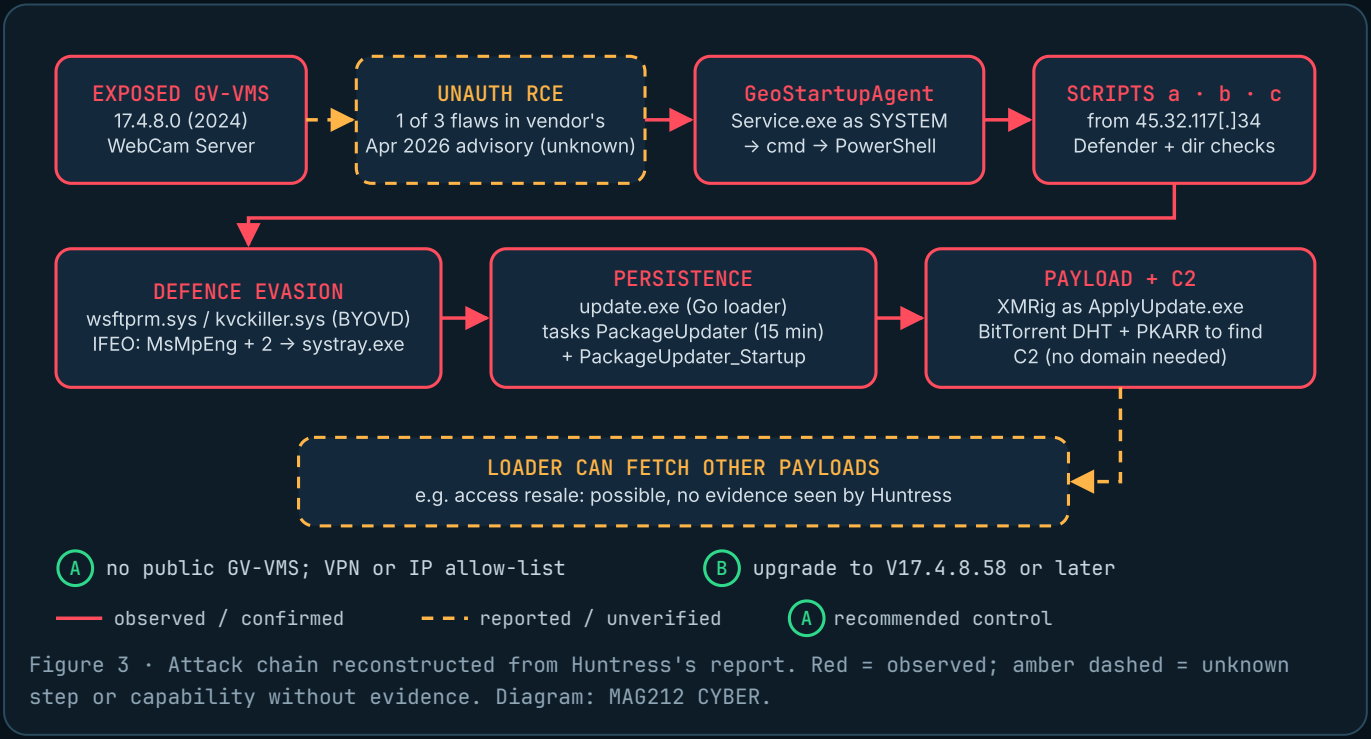


Figure 3 · Attack chain reconstructed from Huntress's report. Red = observed; amber dashed = unknown step or capability without evidence. Diagram: MAG212 CYBER.

Hunting the GeoVision miner

PowerShell 5.1+ | Admin | READ-ONLY | NOT TESTED BY MAG212

GV-VMS · CHILD PROCESSES

```
$svc = Get-CimInstance Win32_Process -Filter "Name='GeoStartupAgentService.exe'"
Get-CimInstance Win32_Process |
  Where-Object { $svc.ProcessId -contains $_.ParentProcessId } |
  Select-Object ProcessId, Name, CommandLine
```

Shows processes currently running under the GeoVision service. Any `cmd.exe` or `powershell.exe` child is suspicious. This only sees live processes: for history, search Sysmon Event ID 1 or Security 4688 (with command-line auditing) for that parent. [10][31]

PowerShell 5.1+ | Admin | READ-ONLY | NOT TESTED BY MAG212

GV-VMS · PERSISTENCE + EVASION CHECK

```
$k = 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options'
'MsMpEng.exe','SecurityHealthService.exe','SecurityHealthSystray.exe' | ForEach-Object {
  Get-ItemProperty "$k\$_" -Name Debugger -ErrorAction SilentlyContinue |
    Select-Object PSChildName, Debugger }
Get-ScheduledTask -TaskName 'PackageUpdater*' -ErrorAction SilentlyContinue |
  Select-Object TaskName, State, @{n='Run';e={$_.Actions.Execute}}
Test-Path "$env:windir\System32\config\systemprofile\update.exe"
Get-CimInstance Win32_SystemDriver | Where-Object { $_.PathName -match 'wsftprm|kvckiller'
}
```

Any output from the first block (a Debugger value on Defender processes), a PackageUpdater task, `True` for the loader path, or a matching driver means the host is compromised. No output is not proof of a clean host. [10][32]

WHAT TO LOOK FOR IN LOGS

- `schtasks /Create` launched by `update.exe`. [10]
- DNS queries straight to 8.8.8.8, 8.8.4.4 or 1.1.1.1 from processes other than the DNS client. [10]
- Outbound UDP DHT traffic (port 6881 or similar) from `WebCamServer.exe`. [10]
- Defender stopped or not starting; sustained high CPU on the VMS host.

False positives: some apps use public DNS resolvers or BitTorrent-style updates. Correlate with the parent process and the GeoVision service before acting.

VERIFY RECOVERY

- GV-VMS at V17.4.8.58 or later; WebCam Server not reachable from the internet.
- Defender running with tamper protection; IFEO keys and tasks gone.
- No traffic to the IoCs; CPU back to baseline; cameras record normally.

CONTAIN AND REMEDIATE

1. Isolate the host and **preserve evidence first** (memory, task XML, the loader) before deleting anything (Huntress). [10]
2. Block the IoCs at the firewall and DNS filter.
3. Remove the IFEO Debugger values, both scheduled tasks, the loader, ApplyUpdate.exe and the driver; re-enable Defender.
4. Reset any credentials stored or used on the host, including the VMS admin and service accounts.
5. Upgrade GV-VMS to V17.4.8.58 or later. If unsure the host is clean, rebuild it. [11]
6. Put management interfaces behind a VPN or a trusted-IP allow-list. [10]

PREVENTION

Put camera and access-control software in the asset inventory and the patch schedule like any other server. Facilities and installers need an IT owner.

REPORT 5 NOV · REPORTED 16 NOV | CVE-2021-44228 · FIXED 2021

NO MALICIOUS RELEASE CONFIRMED

A 2021 bug, a 2026 code-signing breach

Kaspersky's ICS CERT describes how a group it calls BO Team moved from an unpatched vCenter to the server that signs a software vendor's products. The attackers were evicted before any tampered release was confirmed.

> CONTEXT **Dates.** The victim, an unnamed Russian software developer, called Kaspersky in June 2025 after months of compromise. Kaspersky published on 5 November 2026; The Hacker News reported it on 16 November. Kaspersky assesses BO Team (also tracked as Black Owl, Hoody Hyena, Lifting Zmiy) as Ukrainian in origin: its assessment, not independently confirmed. [12][13]

WHAT HAPPENED

After failing to log in to the vCenter web interface, the intruders found a vCenter Server 7.0.3 still vulnerable to Log4Shell and got a root command line. From there they reached the hypervisors over SSH, a second cluster through a host certificate, the GitLab VM and its private key, the Ansible system and, with harvested credentials, the domain controller. [13]

A Windows server that signs the company's commercial builds was 'of particular interest'. Kaspersky says the attackers could have tried to inject code before signing or steal the certificate to sign malware later. [12][13]

WHO IS AFFECTED

- Any vCenter 7.0 below **7.0 Update 3c** that never received the Log4j fix or workaround (VMSA-2021-0028). [14]
- Software publishers whose signing hosts sit in the same domain and trust zone as build and IT systems.
- Customers of the victim: no malicious signed release has been confirmed.

WHY IT MATTERS

Five years after Log4Shell, an unpatched management appliance still opened the door. Virtualization managers are rarely scanned by endpoint tools and often skipped in patch cycles.

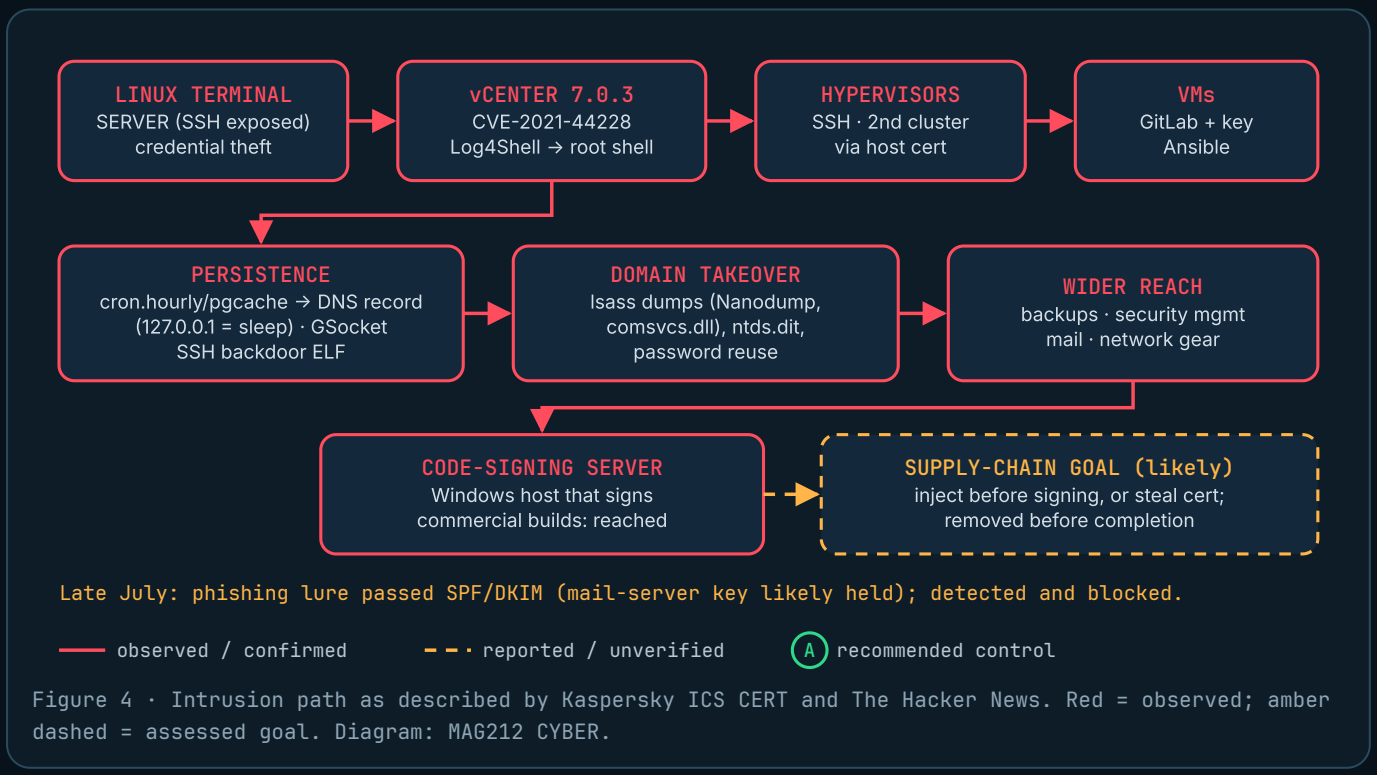


Figure 4 · Intrusion path as described by Kaspersky ICS CERT and The Hacker News. Red = observed; amber dashed = assessed goal. Diagram: MAG212 CYBER.

Check your hypervisor managers, then guard your signing keys

vCenter appliance · bash | root | READ-ONLY | NOT TESTED BY MAG212

VCSA · VERSION + PERSISTENCE

```
vpxd -v
ls -la /etc/cron.hourly/
ls -la /dev/shm/ | grep -i pulse-shm
grep -rIl 'nofrillsdns' /etc /var/spool/cron 2>/dev/null
```

Prints the vCenter build (7.0 U3c is build 19234570) and looks for Kaspersky's persistence artefacts. `pgcache` imitates a PostgreSQL component, so compare with a known-good appliance before deciding. Run the same checks on other Linux hosts and the terminal server, where `/usr/bin/nxnode-login` was altered to capture credentials. [12][13][14]

Linux · zgrep | log read | READ-ONLY | NOT TESTED BY MAG212

LOGS · IOC SWEEP

```
zgrep -iE 'nofrillsdns|proxy-sale' <DNS_OR_PROXY_LOG>*
zgrep -E '193\.3\.23\.236|80\.76\.42\.139' <FIREWALL_LOG>*
```

Searches your DNS, proxy and firewall logs for the domains and IPs Kaspersky published. Replace the placeholders with your log locations; retention limits how far back this can see. [12][13]

KASPERSKY IOCs · 2025 ACTIVITY · VET BEFORE BLOCKING

IPs	193.3.23[.]236 · 80.76.42[.]139
Domains	*.nofrillsdns[.]com (lo1yaizaeghaevarood1ahtaichoota[e|z]) · proxy-sale[.]com
Files	/etc/cron.hourly/pgcache · /usr/bin/nxnode-login (modified) · /dev/shm/pulse-shm-3088612174
Tools	GSocket · Nanodump · comsvcs.dll · Cobalt Strike · Mythic

Source: [12] via [13]. Infrastructure from 2025 may have changed.

WHAT ELSE TO LOOK FOR

- Hourly cron jobs or systemd timers on appliances that you did not install.
- Outbound DNS to free dynamic-DNS providers from servers; GSocket relay traffic.
- lsass access via comsvcs.dll (MiniDump); event-log clearing after a block.

CONTAIN AND REMEDIATE

1. Upgrade vCenter to a supported release (for 7.0, at least U3c, which carries Log4j 2.17); the KB workaround is temporary only. [14]
2. Remove vCenter, ESXi SSH and terminal servers from internet reach; require MFA via a jump host.
3. If artefacts are found: preserve images, then rebuild affected hosts rather than clean them.
4. Reset domain, hypervisor, GitLab and service credentials; stop password reuse across domains.
5. Rotate mail-server DKIM keys if the mail host was in scope.

PROTECT CODE SIGNING · MAG212 ANALYSIS

- Keep signing keys in an HSM or managed signing service, not on a domain-joined server.
- Sign only from the CI pipeline, with approvals and a log of every signature.
- Compare released binaries with reproducible builds or a second build before shipping.
- If a key may be exposed: revoke, re-issue, re-sign and tell customers.

UPDATE TO 15 NOV LEAD | AWS 13 NOV · REPORTED 16 NOV | ATTRIBUTION: MODERATE

AI agents that steal keys to pay their way

STATUS What changed since yesterday. We covered the FBI's ARTEX warning. Amazon now shows one goal: AI provider keys, taken from exposed AI tools and spent on more hunting. Amazon saw only records the agents carried to its decoys and cannot verify their claimed results. [15][18]

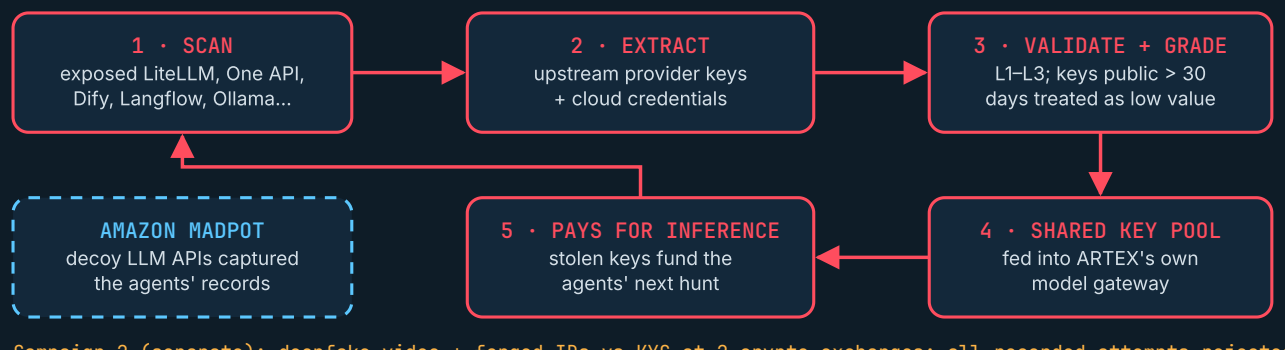


Figure 5 · Campaign 1 loop as described by Amazon Threat Intelligence; steps are the agents' own records. Diagram: MAG212 CYBER.

WHAT HAPPENED

From 3 October to 5 November, Amazon's MadPot sensors posing as LLM APIs received requests from agents running ARTEX. Amazon assesses, with moderate confidence, separate Chinese-nexus groups (simplified-Chinese prompts, China time zones). [15]

WHO IS AFFECTED

LLM gateways (One API, New API, Veloera, Sub2API, LiteLLM) and AI builders (Dify, FastGPT, Langflow, RAGFlow, Open WebUI, LobeChat, Ollama) reachable without authentication or on default credentials. One gateway can expose many upstream accounts. [15][17]

CONTAIN AND REMEDIATE

1. Authentication on every AI gateway and builder; keep them off the internet. [15]
2. Change default admin credentials and master keys; rotate every stored provider key.
3. Patch: Langflow 1.3.0+ fixes CVE-2025-3248. [34]
4. Spend alerts and quotas with each AI provider. [15]

AMAZON IPv4 IOCs · OCT–NOV · VET BEFORE BLOCKING

Campaign 1	104.28.225[.]223 · 31.22.91[.]156 · 150.136.38[.]110 · 128.242.115[.]131 · 216.176.239[.]231
Campaign 2	212.107.28[.]51 · 103.142.140[.]158 · 104.28.251[.]98 · 104.28.251[.]99 · 104.28.219[.]97 · 125.103.213[.]41

Source: [15]. Some sit in shared hosting or proxy ranges; check context before blocking.

Linux/macOS · curl | none | READ-ONLY | NOT TESTED BY MAG212

AI GATEWAY · EXPOSURE CHECK

```
curl -s -m 5 http://<PUBLIC_IP>:11434/api/tags
curl -s -o /dev/null -w '%{http_code}\n' https://<LITELLM_HOST>/v1/models
```

Run from outside your network against hosts you own. Ollama has no built-in authentication, so a JSON model list from the first command means it is open to anyone. A LiteLLM proxy with a master key should return 401 to the second; 200 means no key is required. [33][39]

NETHERLANDS · 1-11 NOV | NO CLICK NEEDED | COMPROMISE OF PHONES: NOT CONFIRMED

The ad that came for old iPhones

Malicious code slipped into one advertising partner's tag reached readers of at least 12 Dutch news and lifestyle sites, recorded their visits and tried to exploit iPhones that had missed security updates.

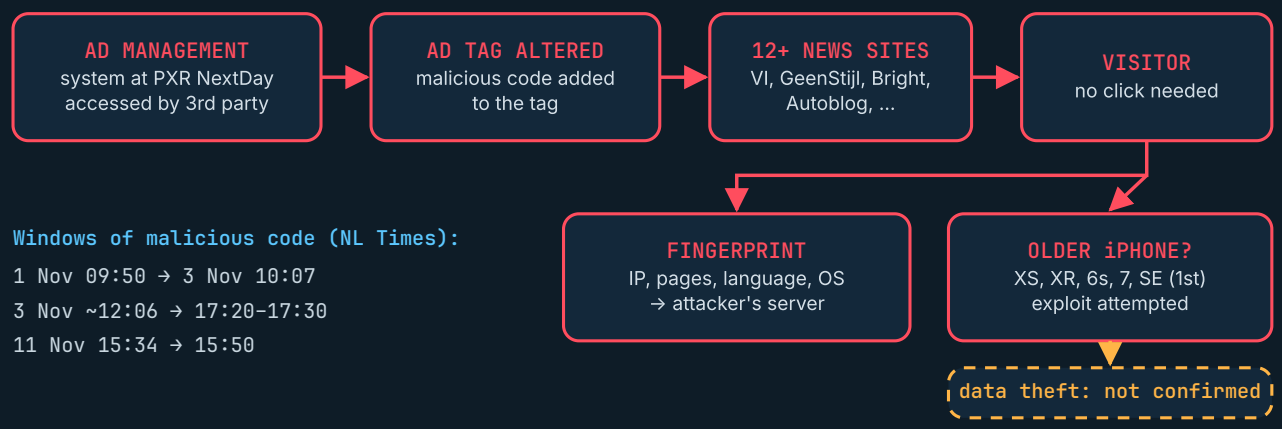


Figure 6 · Chain as described by the publishers via NL Times and TPO. Times are local. Diagram: MAG212 CYBER.

WHAT HAPPENED

Publisher VI says an unauthorised third party accessed the advertising management system and inserted code into an ad tag; the code has been removed and the weakness fixed. All affected sites use PXR NextDay, which manages ads for about 150 sites. NL Times lists 12 sites; TPO counts at least 14 Dutch sites and one Belgian. [19][21]

The code did two things: it collected IP address, pages visited, language and operating-system details and sent them to an attacker server, and it tried to exploit security flaws on certain older iPhones. Successful exploitation could expose passwords, messages, photos, contacts and wallet keys, but no infected phone has been confirmed. [19][20]

UNKNOWN

Which iOS flaws and versions were targeted, who is behind it, and whether any data left a phone. The reports name no CVE and no police or CERT involvement.

IF YOU VISITED ON AN OLDER iPHONE

1. Install the latest iOS update offered for the device (Settings → General → Software Update). [19][35]
2. Change passwords stored on the phone, from a different trusted device.
3. Turn on two-step verification and watch for odd sign-ins.
4. Crypto wallet on the phone: move funds to a new wallet with a new recovery phrase made on a secure device. [19]
5. A phone that no longer gets updates should not hold banking, work or wallet apps; high-risk users can enable Lockdown Mode. [36]

FOR PUBLISHERS AND AD TEAMS

- Treat ad-server and tag-manager logins as admin access: MFA, named accounts, alerts on tag edits.
- Review change history for unexpected script sources; use Content Security Policy where ads allow.
- Agree incident-notification terms with every ad partner.

Device list and advice as published by the sites via NL Times [19]. Publisher and ad-team controls are MAG212 recommendations.

Also today

CISA KEV · DUE TODAY, 16 NOVEMBER

CVE	PRODUCT	ADDED	DUE	MAG212
CVE-2026-114713	UnrealIRCd	13 Nov	16 Nov	Daily 15 Nov p.10
CVE-2026-123039	Check Point (Gaia)	13 Nov	16 Nov	Weekly 14 Nov p.04–05

Both were added on 13 November with a three-day window for US federal agencies. If you run either, confirm the fix is in and the log hunt is complete; see our earlier coverage for steps. [26][27]

RETAIL · AUSTRALIA

Coles investigates a cyber incident

Coles Group says it is investigating a cyber security incident with outside experts and the Australian Cyber Security Centre. Stores and online shopping are open, and so far it has found no evidence that customer, team or supplier data was compromised. A small number of Liquorland click-and-collect orders have problems; Coles has not linked them to the incident. No attacker or entry method has been named. [22][23]

DISCLOSURE POLICY

Project Zero: details out 90 days after report, fixed or not

Google Project Zero has replaced its '90 + 30' rule with 'Full X': bug details are published X days after the report whatever the fix status. X is 90 now, 60 from 2 February 2027 and 30 from 3 January 2028. The grace period goes. In-the-wild bugs follow Google's separate policy. The team cites faster, AI-assisted exploitation. [24][25]

EMAIL SECURITY

Rspamd 4.3.0 stops forwarders softening DMARC rejects

Rspamd now trusts an ARC forwarder only for what it vouches for and needs the forwarder's own dmarc=pass before changing a DMARC result. It also fixes unescaped sender text in Authentication-Results, a worker crash from one unauthenticated HTTP request, and a milter-proxy use-after-free in 4.0.0–4.2.3. Test local scores before upgrading. [28]

ENDPOINT MANAGEMENT

Microsoft previews Intune remote lock for Windows

Admins can lock a lost or stolen Windows 10/11 or Server 2016–2022 device without wiping it, using a custom profile with LockState. The lock survives restarts and works offline. It does not disable the account, isolate the network or block WinRE or USB boot, so keep BitLocker on and revoke sessions in Entra ID. [29]

MAG212 VIEW ON PROJECT ZERO

Shorter, fixed disclosure clocks will put more unpatched-bug details in public. For defenders the practical change is the same as this issue's theme: you need an owner and a patch path for every product you run, including the 'boxes' outside IT, because the time between disclosure and exploitation is shrinking.

Your work list for today

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

WHEN	TEAM	ACTION	SEE
TODAY	OT / facilities	Remove internet exposure of Danfoss AK-SM800A and similar controllers, including modems; keep monitoring alive.	p.03-04
TODAY	Vuln mgmt	Close UnrealIRCd CVE-2026-114713 and Check Point CVE-2026-123039 (KEV due 16 Nov).	p.11
TODAY	SOC	Run the GeoVision child-process, IFEO and task checks on every GV-VMS host.	p.06
48 H	Platform / AI	Authenticate or unpublish LiteLLM, Dify, Langflow, Ollama; rotate stored provider keys; set spend alerts.	p.09
48 H	Virtualization	Confirm every vCenter is on a fixed build (7.0 U3c+ or newer line); remove internet SSH; check cron.hourly.	p.08
THIS WEEK	Engineering	Move code-signing keys to an HSM or signing service; sign only from CI with approvals and logs.	p.08
THIS WEEK	Web / marketing	MFA and change alerts on ad servers and tag managers; review recent tag edits.	p.10
THIS WEEK	IT / MDM	Find phones that no longer receive iOS updates; keep wallets and work apps off them.	p.10, 13
THIS MONTH	Leadership	Name an owner for every non-IT device on the network: fridges, cameras, building systems.	p.13

ONE-PAGE HUNT SHEET

Windows	Children of `GeoStartupAgentService.exe`; IFEO Debugger on MsMpEng.exe; tasks `PackageUpdater*`.
Linux / VCSA	`/etc/cron.hourly/pgcache`; DNS to `nofrillsdns`; GSocket.
Network	UDP DHT from camera servers; LLM API calls from servers; inbound to controller web UIs.
Cloud / AI	Unexpected AI provider spend; new keys in gateways; Amazon's 11 IPs.

BEFORE YOU CLOSE A TICKET

- Re-test exposure from outside the network, not from the admin's desk.
- Keep evidence (images, logs, task XML) before you clean.
- Rotate any credential or key the box could read.
- Record the owner and patch path in the asset inventory.

COMMAND SAFETY

Every command in this issue is read-only and was checked against vendor documentation, but none was run by MAG212. Test in a lab or on one host first, run with the least privilege shown, and replace placeholders in <ANGLE_BRACKETS> with your own values.

Who owns the box?

A five-minute lesson for managers, facilities staff and anyone with a work phone.

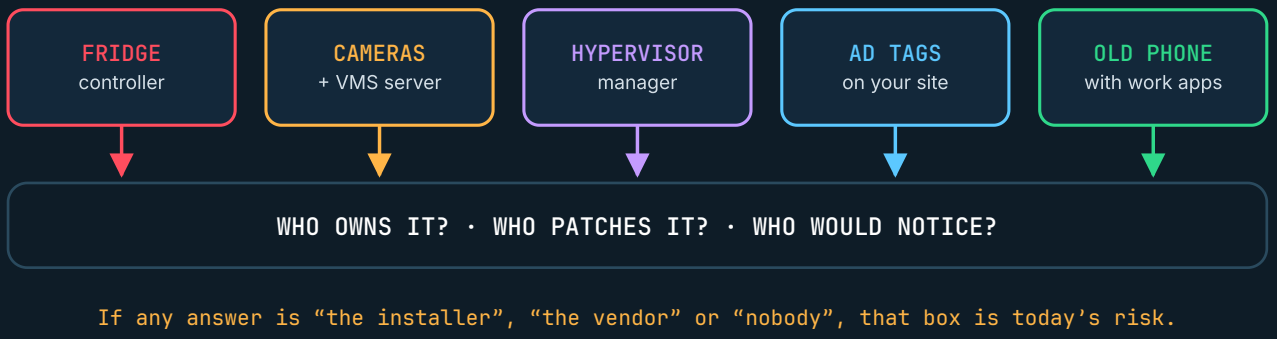


Figure 7 · Conceptual illustration. MAG212 CYBER.

FOR BUSINESS LEADERS

- Ask for a list of every device that connects to the internet, including ones run by contractors (refrigeration, CCTV, building management).
- Each one needs a named owner, a way to update it and a way to know if it misbehaves.
- Contracts with service firms should say how they connect remotely, how fast they patch and how they tell you about incidents.
- Budget to replace equipment that can no longer be updated.

FOR EMPLOYEES

- Install phone and laptop updates the day they arrive. Today's iPhone attack needed no click.
- If your phone no longer gets updates, keep banking, work and wallet apps off it.
- Odd behaviour from equipment (a fridge alarm, a slow camera PC, a hot server) is worth reporting.
- Never connect a modem, router or camera to the work network without IT.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Which of our devices can be reached from the internet, and how do we know?
2. Which supplier can log in to our equipment, and through what?
3. If a fridge, camera or ad tag were tampered with tonight, who would see it first?

WHY IT MATTERS

In October, attackers used fridge controllers that were reachable from the internet to spoil stock in hundreds of stores. This week researchers showed the newest firmware is still open to attack without a login. The cheapest protection is still the simplest one: if a device does not need the internet, take it off. [1][30]

Sources

[1] The Hacker News · 16 Nov · Six unpatched Danfoss refrigeration controller flaws could allow remote takeover without login

[2] Midnight Blue · Nov · Multiple pre-authentication RCE vulnerabilities in Danfoss AK-SM800A

[3] CCB Belgium · Nov · Warning: six new Danfoss vulnerabilities in refrigeration controllers, immediate action

[4] NCSC Ireland · 13 Nov · New vulnerabilities in refrigeration controllers (advisory PDF)

[5] BSI · Nov · Cybersicherheitswarnung: Danfoss AK-SM800A (PDF)

[6] BSI · 13 Nov · Press release on Danfoss refrigeration controllers (corrected)

[7] Danfoss · page · Danfoss security advisories (coordinated vulnerability disclosure)

[8] Cooling Post · Nov · Belgium warns of new Danfoss controller vulnerabilities

[9] Claroty Team82 · Aug · Freeze the controller, defrost the food: vulnerabilities in Danfoss refrigeration controllers

[10] Huntress · 13 Nov · GeoVision camera software exploited to deploy XMRig cryptominer

[11] Help Net Security · 16 Nov · Unpatched GeoVision camera software gave cryptojackers a side door into 13 organizations

[12] Kaspersky ICS CERT · 5 Nov · Supply chain attack: BO Team in a software developer's infrastructure

[13] The Hacker News · 16 Nov · BO Team exploits Log4Shell in VMware vCenter, compromises Russian firm's code-signing server

[14] Broadcom (VMware) KB 318925 · KB · Workaround instructions to address CVE-2021-44228 and CVE-2021-45046 in vCenter Server

[15] AWS Security Blog · 13 Nov · Amazon Threat Intelligence observes threat actors running cybercrime campaigns with ARTEX AI agents

[16] Cybernews · 16 Nov · AI agents stole API keys to bankroll a month of autonomous cybercrime, Amazon warns

[17] Tbreak · 16 Nov · AI agents are hunting exposed LiteLLM and Dify tools for API keys

[18] MAG212 CYBER · 15 Nov · FBI ARTEX FLASH: AI agents and autonomous intrusions, a defender's guide

[19] NL Times · 15 Nov · At least 12 Dutch websites warn of malicious ad code that tried to hack old iPhones

[20] Cybernews · 16 Nov · Hackers turned at least 12 Dutch websites into traps for older iPhones

[21] TPO · 15 Nov · Malware via advertenties treft veertien Nederlandse websites

[22] Coles Group · 16 Nov · Updates: cyber security incident

[23] CybersecurityNews · 16 Nov · Australia's supermarket chain Coles investigates cyber security incident

[24] Google Project Zero · 13 Nov · Disclosure policy update (Full X)

[25] Help Net Security · 16 Nov · Google Project Zero will disclose bugs after 90 days, fixed or not

[26] CISA · 13 Nov · CISA adds two known exploited vulnerabilities to catalog

[27] MAG212 CYBER · 15 Nov · UnrealIRCd CVE-2026-114713 exploited: patch by November 16

[28] Help Net Security · 16 Nov · Rspamd 4.3.0 stops forwarded mail from softening DMARC rejects

[29] Help Net Security · 16 Nov · Microsoft previews remote lock for lost or stolen Windows devices

[30] MAG212 CYBER · 14 Nov · Cold-chain sabotage: France blames IRGC-linked SHAHID KAVEH (Weekly)

[31] Microsoft Learn · docs · Get-CimInstance (CimCmdlets)

[32] Microsoft Learn · docs · Get-ScheduledTask (ScheduledTasks)

[33] Ollama · docs · API reference (GET /api/tags)

[34] NVD · record · CVE-2025-3248 (Langflow, fixed in 1.3.0)

[35] Apple · page · Apple security releases

[36] Apple · page · About Lockdown Mode

[37] CybersecurityNews · 15 Nov · Researchers find six 0-days allowing unauthorized takeover of supermarket refrigeration systems

[38] CRA Decoded · 15 Nov · Six unpatched flaws in the Danfoss controller behind the supermarket attacks (11–13 Nov timeline)

[39] LiteLLM · docs · Proxy: virtual keys and master key

HOW WE VERIFIED THIS ISSUE

- Primary sources read where reachable: Midnight Blue, Huntress, Kaspersky (via THN's detailed summary), AWS Security Blog, Google Project Zero, Coles Group, CISA, Broadcom KB.
- Agency advisories (CCB, NCSC-IE, BSI) are cited as linked by The Hacker News; we did not read the PDFs in full. Dutch ad-tag details rely on publisher statements reported by NL Times and TPO.
- No command in this issue was executed by MAG212. Syntax was checked against vendor documentation.
- Not used: an unverified Apache Shiro CVE listed by an aggregator, and an Uber breach report we could not confirm.

Read.
Verify.
Defend.

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

SUBSCRIBE FREE

Get every issue in your inbox

cyber.mag212.com/subscribe-free

MAG212 ATLAS · LIVE DEMO

Map every network before you test it

demo.atlas.mag212.com

WORK WITH MAG212 CYBER

Penetration testing
Find the forgotten edge before someone else does.

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

Training
For staff, IT teams, leaders and schools.

cyber.mag212.com/services

Watch the Atlas walkthrough: youtu.be/j27B5g3viKw

MAG212 CYBER

Daily · 16 November 2026
Understand the threat. Build the defense.