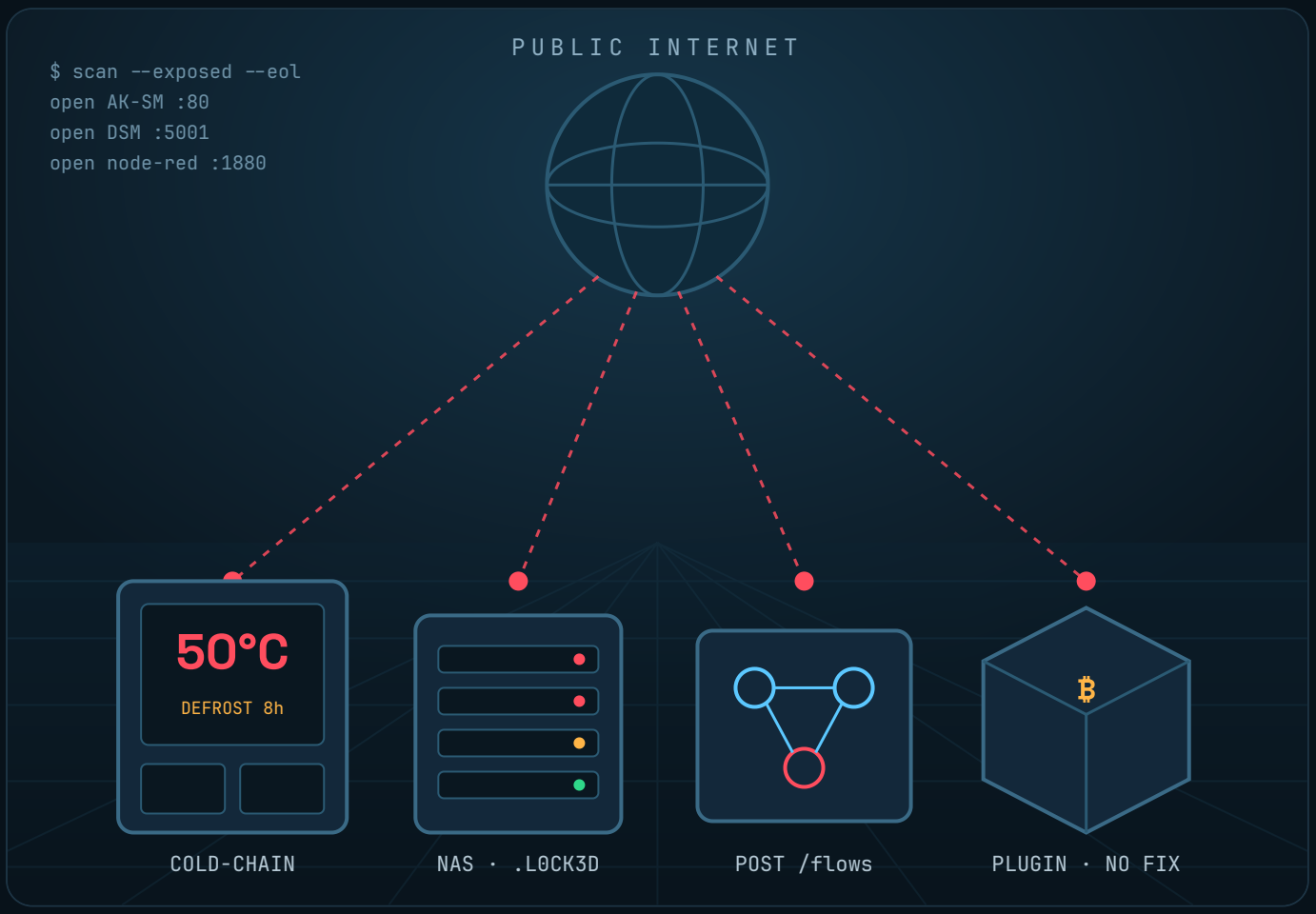
MAG212
CYBER

DAILY INTELLIGENCE
Tuesday, 3 November 2026
TECHNICAL EDITION · 14 PAGES



COVER STORY · EXPOSURE MANAGEMENT

The Forgotten Edge

Freezers set to 50°C, end-of-life NAS boxes, open Node-RED gateways and an abandoned payment plugin. This week attackers worked through the equipment nobody watches.

03 **Cold chain:** two waves of freezer attacks across Europe

05 **Synology:** why the SA-24:20 patch is not enough

06 **Node-RED:** 11 weeks from patch to exploitation

10 **$6.43B:** the FBI names Binance's thieves

Cover: conceptual illustration

Exposure is the vulnerability

None of this issue's lead stories needed a fresh zero-day. The freezer attacks in France and northern Europe hit refrigeration supervisors that were reachable from the internet, including models out of support since 2016 and 2021. Synology's ransomware victims run end-of-life DSM. Siemens fixed the IoT2050 Node-RED flaw on 11 August; exploitation started on 30 October. The CryptoPayment Gateway plugin was pulled from WordPress.org on 28 August and still has no fix.

The lesson for defenders is an order of work: find what is exposed, take it off the internet, then patch. This issue gives you the facts, the commands and the closure evidence for each.

50°C
Defrost setpoint used in both freezer waves

11 wks
Siemens patch to first Node-RED exploitation

0
CVEs officially tied to the freezer attacks

$6.43B
Binance theft the FBI attributes to TraderTraitor

INSIDE THIS ISSUE

03 Two waves of 50°C freezer attacks
04 Cold-chain response playbook
05 Synology: two advisory generations
06 Node-RED: the attack chain
07 Node-RED lab: harden and investigate
08 WordPress: a payment plugin with no fix
09 Identity and mobile watch
10 The crypto weekend
11 Tech briefs: LXD, Langflow, x.cpe
12 The action desk
13 Source register

VERIFICATION DESK

We checked yesterday's early reporting against primary sources. Four points changed:

Coop. Coop told Aftonbladet six stores were affected. It did not tell Reuters about "tampering"; an unnamed store blamed hackers.

Synology. A second vendor ties the C3RB3R ransomware to newer SA-26:13 flaws. Patch to SA-26:13 builds, not just SA-24:20.

Linux DDoS. The weekly recap names one botnet, Kairos, not several.

RISK:STATION. CVE-2024-10443 belongs to Synology Photos (SA-24:19), not SA-24:20.

HOW TO READ THIS ISSUE

Vendor and CERT advisories anchor every product, version and fix. Command panels marked ILLUSTRATIVE use standard tool syntax for systems you are authorized to manage; test them first. Interface panels are simplified recreations for explanation, not vendor screenshots, and the illustrations are conceptual. Figures from a single source are attributed in the text.

Verification desk sources: [3] [9] [11] [17] · cyber.mag212.com

Two waves of 50°C defrost attacks hit Europe's cold chain

Attackers reached internet-facing refrigeration supervisors, the Copeland, Danfoss and Dixell models CERT-FR lists, and set cases to defrost for hours. Nobody has claimed either wave, and no CVE has been tied to them.

TIMELINE · 2026

AUG	OCT 11–12	OCT 12 · 13 · 16	NOV 1–2	NOV 3
Claroty finds 2,765 exposed AK-SM 800A units	Wave 1 hits hundreds of French supermarkets	CERT-FR alert ALE-012 published, then updated twice	Wave 2 hits five more countries	No attribution, no new advisory

Wave 1: France

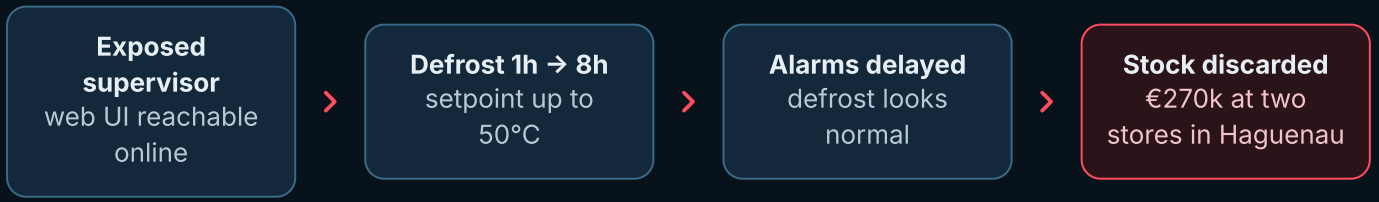
Overnight on 11–12 October, controllers were switched to continuous defrost at setpoints up to 50°C. AFP counted at least 300 Intermarché and Netto stores, plus about 100 Coopérative U and 80 Carrefour sites. Intermarché's CEO put losses at tens of millions of euros in a day.

> "Quite a lot of exposed operational technology devices in Sweden."
>
> John Billow, head of Sweden's national cybersecurity centre, via Al Jazeera

Wave 2: northern Europe

COUNTRY	REPORTED IMPACT
Sweden	ICA: "a limited number" of stores. Coop: six stores, per Aftonbladet. Axfood: a home-delivery hub near Gothenburg.
Ireland	SuperValu: 13 of 223 stores, one refrigeration model.
Belgium · Lux.	Dozens of Ahold Delhaize stores (Belga). Five Spar shops (Colruyt).
Estonia	At least one chain, set to 50°C.
Netherlands	Reported by Tom's Hardware only.

HOW A DEFROST ATTACK DAMAGES STOCK · SCHEMATIC



WHAT WE DON'T KNOW

Who did it, and which vendor and model were hit in wave 2. European states blame Moscow for other infrastructure incidents; Russia denies involvement. Claroty's Danfoss and Copeland flaws are context, not a confirmed entry point.

Restore trust before remote access

CERT-FR's sequence for refrigeration supervisors, with the checks we would add.

Store supervisor · Case 14 · Defrost settings — 3 DEVIATIONS

PARAMETER	APPROVED BASELINE	OBSERVED	STATUS
Max defrost duration	60 min	480 min	Changed
Defrost termination	8 °C	50 °C	Changed
Web interface	VPN only	Public IP	Exposed
Security level	Strict	Standard	Review

Simplified recreation for illustration, not a vendor screen. Example values echo the 1h → 8h, 50°C settings reported in France.

CERT-FR · UNITS NOT YET COMPROMISED

1. Take every affected or public-IP unit off the internet. Check your insurance contract before cutting data to the refrigeration contractor.
2. Review the full configuration, especially defrost schedules.
3. Restore access only through a secure VPN. Filtering contractor IPs is a stopgap.
4. Danfoss: update firmware, set the security level to **Strict**, change default passwords.

UNITS ALREADY COMPROMISED

Reboot (Danfoss) or factory-reset, then reconfigure before the unit returns to service. A reset removes persistence but not the flaw: CERT-FR warns that unpatched end-of-life units left online face a "very high probability" of compromise.

AK-SC355 and AK-SM800 units cannot be patched. Isolate them from the network and plan replacement.

Food disposition belongs to the site's food-safety process, confirmed with independent thermometers, not to a recovered dashboard.

TARGET ACCESS DESIGN · MAG212 RECOMMENDATION

Contractor named account + MFA › **VPN gateway** time-limited session › **OT firewall** one rule, one controller › **Supervisor** no public address

Separate log collector for logins and configuration changes

Independent alarm path so a hijacked supervisor can't silence warnings

EVIDENCE THAT CLOSES THE TICKET

- ✓ Asset list with firmware
- ✓ Approved settings restored
- ✓ Deny rule tested
- ✓ Vendor accounts reviewed
- ✓ Alarm test recorded
- ✓ External re-scan shows no UI

Synology's warning spans two patch generations

On 29 October Synology said attackers are exploiting "a vulnerability first patched in December 2024" to encrypt end-of-life DSM systems. It cites SA-24:20 and SA-26:14 but names no CVE; another vendor points to newer flaws.

SA-24:20

Pwn2Own 2024 · fix Dec 2024

Cited by Synology's 29 Oct warning

CVE-2024-10441 · 9.8 · unauth RCE
CVE-2024-50629 · 5.3 · file read
CVE-2024-10445 · 4.3 · file write

7.2.2-72806-1 · 7.2.1-69057-6
7.2-64570-4 · 7.1.1-42962-7
6.2.4-25556-8

SA-26:13

published 18 Sep 2026

Tied to the attacks by vendor 360, via Gridinsoft

CVE-2026-13639 · 9.8 · unauth
CVE-2026-13684 · 9.8 · unauth

Patch to these builds or later:

7.4-90075 · 7.3.2-86009-4
7.2.2-72806-9 · 7.2.1-69057-12

FAMILY (PER 360)
C3RB3R
A Cerber variant

EXTENSION
.L0CK3D
With a zero, not an O

RANSOM NOTE
read-me3.txt
Synology names no family

PHP2Shell is a separate fix

Synology extended PHP2Shell fixes (CVE-2026-109618/-109619) to end-of-life DSM 7.2 to 6.2; MailStation needs a manual update and older DSM gets none. HKCERT notes PHP2Shell's role is unconfirmed.

If files are already encrypted

HKCERT's advice: disconnect the NAS and pause sync and backup jobs. Keep the ransom note, samples and logs. Don't reset or format the device, and don't count on paying.

Control Panel › Update & Restore

Installed	DSM 7.2.1-69057 Update 6
Needed for SA-26:13	7.2.1-69057-12+
External access	5001 forwarded

Patched for SA-24:20 only. Still exposed to SA-26:13.

Simplified recreation, example values

admin@nas:~$ · SSH, read-only checks — ILLUSTRATIVE

```
# Which DSM build is installed?
$ cat /etc.defaults/VERSION | grep -E 'productversion|buildnumber|smallfixnumber'
# Any C3RB3R artefacts on the first volume?
$ find /volume1 \( -name 'read-me3.txt' -o -name '*.L0CK3D' \) 2>/dev/null | head
```

Node-RED: when the deploy API is a shell

Siemens fixed a missing-authentication flaw in the Node-RED interface of its SIMATIC IoT2050 Advanced gateway on 11 August. Eleven weeks later, VulnCheck's decoy sensors caught the first attempt to use it.

CVE
2026-58115
CWE-306 · SSA-834709

CVSS 3.1 · 4.0
10.0 · 10.0
"maximum privileges"

AFFECTED
IoT2050 Advanced 6ES7647-0BA00-1YA2, < V4.3.4.1 with Node-RED

FIX
V4.3.4.1+
or remove / harden Node-RED

11 AUG Siemens advisory and fix

27 OCT VulnCheck ships detections

30 OCT First hit on a decoy

1 NOV 16 events from one IP

2 NOV VulnCheck publishes

OBSERVED ATTACK CHAIN · FROM VULNCHECK TELEMETRY

POST /flows — no auth · curl/8.5.0 →
inject → exec — fires once after ~1 s →
base64 | sh — HTTP 200 + revision →
/dev/shm/.b — setsid, else nohup →
/tmp/.s — staged from wget.sh →
/tmp/.kworker — second binary →
http in /cmd → exec — persistent web shell inside the flows

INDICATORS · DEFANGED

Source	4.201.105[.]116 Microsoft AS8075
Payload 1	85.215.73[.]250:8080 /bot-linux-amd64 · /wget.sh
Payload 2	45.194.90[.]57:38472 /.sys_update
Files	/dev/shm/.b · /tmp/.s · /tmp/.kworker

READ THE EVIDENCE CAREFULLY

This is decoy telemetry. No compromise of a real Siemens device is confirmed, and the payloads were not analysed. The same IP probed eight other CVEs, including in Apache Solr, Gitea and MLflow, so VulnCheck reads it as opportunistic scanning.

The flaw is in VulnCheck's KEV list but not CISA's. Because the attack uses Node-RED's normal deploy API, **any internet-facing Node-RED without adminAuth** is just as exposed.

Lock the editor, then look for what is already inside

For any Node-RED you run, on an IoT2050 or anywhere else. Work only on systems you are authorized to manage.

Flow editor · gateway-07 · Flow 1 — 2 UNAPPROVED FLOWS



Simplified recreation of the two flow patterns VulnCheck describes. Times are an example, not telemetry. Legitimate automations can use exec too, so check change records before calling one malicious.

~/.node-red/settings.js — NODE-RED DOCS

```
adminAuth: {
  type: "credentials",
  users: [{
    username: "admin",
    password: "<bcrypt hash>",
    permissions: "*"
  }]
},
// protects http-in routes like /cmd
httpNodeAuth: {
  user: "user",
  pass: "<bcrypt hash>"
},
https: { key: ..., cert: ... }
```

Make each hash with `node-red admin hash-pw`. TLS alone does not stop anyone deploying a flow.

root@gateway · triage — ILLUSTRATIVE

```
# 1. Is the admin API locked?
$ curl -s -o /dev/null -w '%{http_code}\n' \
    http://127.0.0.1:1880/flows
  expect 401, not 200
# 2. Listeners and process tree
$ date -u; ss -lntp
$ ps -eo pid,ppid,user,lstart,args \
    --forest
# 3. Reported drop paths
$ ls -la /dev/shm/.b /tmp/.s /tmp/.kworker
# 4. Service log since first attempt
$ journalctl -u nodered \
    --since 2026-10-30 --utc
```

Unit names vary by appliance. Copy suspicious files; never run them.

AUDIT

Export flows from an approved session, hash the export and compare it with your version-controlled baseline.

IF EXECUTION IS CONFIRMED

Isolate, preserve evidence, rebuild from vendor media and rotate every credential the gateway held.

DON'T JUST REBOOT

A malicious flow is saved in the project and starts again on boot. Patch and restrict access before reconnecting.

A payment plugin with no fix, and attackers knocking

CryptoPayment Gateway (slug `cryptopayment-gateway`) was pulled from WordPress.org on 28 August. On 3 November The Hacker News reported that Defused Cyber is seeing exploitation attempts against sites that still run it, from infrastructure sold as "Anonymous KYC-Free VPS Hosting".

CVE	CVSS	VERSIONS	FIX
2026-81648	10.0	1.2.1 - 1.2.2	None
CWE-284 · WPScan	no login needed	1,845 lifetime downloads	remove the plugin

ONE MISSING CHECK, FOUR ACTIONS · FROM WPSCAN'S ADVISORY

Anonymous request
no session, no nonce

›

`vendor/cryptd/ajax.php`
router with no authorization check

›

- `get-settings` read config
- `save-settings` swap payout details
- `encryption` wallet secrets in clear
- `delete-file` arbitrary deletion

Telling detail: the sibling router `ajax1.php` rejects the same request with "Security error". The guard existed; it was missing here.

Why ”deactivate” is not enough

The router is a PHP file the web server runs directly, so it answers even when WordPress no longer loads the plugin. Delete the plugin's files through a controlled change, and don't confuse this slug with other crypto payment plugins.

Then assume the keys are gone

Rotate API credentials from a clean machine. A stolen blockchain private key stays valid after any password change: move funds to fresh keys, with qualified help if needed. Compare payout addresses, admin accounts and scheduled tasks with a trusted baseline.

deploy@web · WP-CLI — ILLUSTRATIVE

```
# Is it installed?
$ wp plugin list \
    --name=cryptopayment-gateway \
    --fields=name,status,version
# Keep a copy for evidence, then delete
$ wp plugin delete cryptopayment-gateway
# Look for hits on the router
$ grep -E 'cryptd/(ajax|upload)\.php' \
    /var/log/nginx/access.log
# Check core and plugin integrity
$ wp core verify-checksums
$ wp plugin verify-checksums --all
```

Access logs rarely keep POST bodies. A 200 response alone does not prove theft, and no hits do not prove safety.

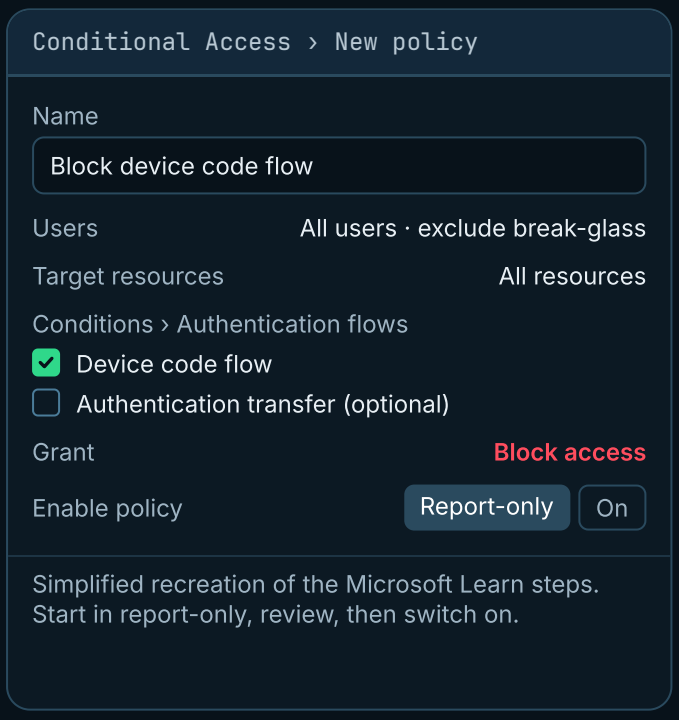
Phishing that uses the real Microsoft sign-in page

The weekly recap's identity story is MadApe, a device-code phishing kit Group-IB first saw on 7 January 2026. It sends business-themed PDF lures and fake document-sharing pages. The domain the victim types into is genuine, so checking the URL doesn't help.

HOW DEVICE-CODE PHISHING WORKS

1 · Attacker requests a device code › **2 · Lure** PDF or fake share page › **3 · Victim** enters code on the real page › **4 · Tokens** access + refresh to attacker

Background: Microsoft documented this tradecraft with Storm-2372 in February 2025 and in July 2026 assessed the group as an initial-access sub-cluster of Midnight Blizzard. The recap also reports M365 token-replay attacks on 97 accounts at 79 organizations.



Simplified recreation of the Microsoft Learn steps. Start in report-only, review, then switch on.

PS · Microsoft Graph — ILLUSTRATIVE

```
# After a confirmed compromise:
# kill refresh tokens and sessions
PS> Revoke-MgUserSignInSession `
      -UserId user@contoso.com
```

A password reset alone may not end sessions the attacker already holds. Microsoft also advises phishing-resistant MFA and blocking legacy authentication. Review device-code sign-ins alongside new device registrations and mailbox rule changes.

ALSO NAMED IN THE RECAP

Skyw4lker and EvilTokens appear only as a headline and a link. We attribute no details to them.

Linux DDoS: Kairos

Nozomi Networks

A Go-based bot that got in over Telnet with root and an empty password. On command it opens hundreds to thousands of TCP connections to a target. Its size and targets are unknown. It is the only Linux DDoS botnet the recap names.

Do now: disable Telnet; set root passwords on Linux and IoT devices.

Android

17,960 devices

uCreator, commercial spyware aimed at wallet and messaging users in China and Southeast Asia, can clone WeChat accounts. The **CyberDakait** cluster of Indian banking trojans (GhostBat and others) hit at least 17,960 devices and intercepted about 7.6M texts.

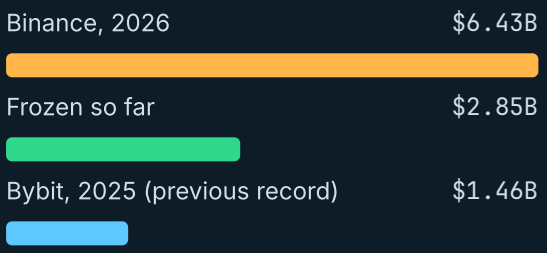
Do now: managed app stores; review sideloading and accessibility permissions.

The FBI names Binance's thieves, and two more platforms bleed

LARGEST CRYPTO THEFT ON RECORD

$6.43B

across 11 blockchains, per The Hacker News. The FBI says "more than $6.3B".



Binance and North Korea's TraderTraitor

Over the weekend of 31 October–1 November, the FBI, the Secret Service and IRS-CI attributed the theft to TraderTraitor. Tether, Circle, Ripple, Arbitrum and Optimism froze about $2.85B. The FBI published the attackers' wallet addresses, but Elliptic counted about 12,000 wallets and warned that static lists can't keep pace with automated laundering.

The group's known way in is people, not protocols: fake recruiters and trojanized Terraform providers aimed at developers.

Do now: screen flows continuously against the FBI list; train engineers on recruiter and tooling lures.

Polymarket: drained through a monitoring script

attack 29 Oct

DebugBear script third-party performance tag › **Domain hijacked** registrar or DNS: reports differ › **Wallet drainer** served on polymarket.com › **$2.7M · 33 wallets** under an hour; $3.9M refunded

DebugBear blames its domain registrar, according to The Record; SecurityWeek's headline calls it a DNS hijack. Either way, a script your page trusts is code you don't control. Pin it with Subresource Integrity, restrict where scripts load from, self-host anything critical, and watch your vendors' registrar and DNS records.

index.html ILLUSTRATIVE

```
<script src="https://cdn.vendor/rum.js"
  integrity="sha384-<hash>"
  crossorigin="anonymous"></script>
```

Mercado Bitcoin

1–2 Nov

Latin America's largest crypto platform, with about 4.5M customers, halted deposits and withdrawals. Blockchain firms say more than $46M left late on 1 November; the company has not confirmed the figure. About $6.5M has been frozen, and experts dispute its claim that customers weren't harmed.

Chainalysis

disclosed 30 Oct

An intruder using "offensive agentic techniques" exposed user IDs, names, emails and organization role labels. Passwords, MFA secrets and investigation data were not found to be accessed, and the company says the incident is unrelated to Binance.

Also this weekend

TAKEDOWN 2 Nov

Google disrupts a 1.3M-device Android TV botnet

The x.cpe backdoor sat in the firmware of cheap TV boxes. Google says it is "highly confident" maker Videostrong installed it on purpose and has banned it from certified Android.

Do now: match boxes against Synthient's 182-model list and discard them. The backdoor reinstalls on restart.

CVSS 10.0 1 Nov

LXD, MicroCloud and Incus trust a public certificate

CVE-2026-112816 lets an attacker authenticate as a trusted client using only its public certificate. Fixed in LXD 6.10.1 / 5.21.9 / 5.0.11 / 4.0.15, MicroCloud 3.4.1 / 2.1.5 and Incus 7.6.0. Not exploited; Ubuntu-archive LXD is unaffected.

```
$ snap refresh lxd && snap list lxd
$ lxc config get core.https_address
```

CVSS 9.8 · AI TOOLING 2 Nov

Langflow: two unauthenticated RCE flaws

CVE-2026-93680 and CVE-2026-110186 hit the AI agent builder from 1.0.0 to 1.12.8. Auto-login is on by default in 1.12.8, and a public Metasploit module exists for the first flaw. No in-the-wild use is reported yet.

Do now: upgrade to 1.13.0 and keep Langflow off the internet.

ZERO-DAYS 2 Nov

Ivanti patches two more Connect Secure zero-days

SecurityWeek reports two more exploited flaws in the same attack chain; we could not yet confirm the CVE IDs or versions. Ivanti's Integrity Checker missed the earlier chain because it ran in memory.

Do now: apply Ivanti's latest release and hunt beyond the Integrity Checker.

SPYWARE 2 Nov

Apple warns users in 99 countries

A new round of mercenary-spyware threat notifications. Apple names no actor or vendor. Anyone who receives one should treat the device as targeted and consider Lockdown Mode.

EDUCATION · CLAIM 2 Nov

BYOD gang claims Michigan State

The gang claims data on 1.3M people. The claim is unverified; MSU forced a campus-wide password reset on 1 October and says its central Active Directory was not shown to be compromised.

IN BRIEF · HEADLINES ONLY

Revolve discloses a breach affecting at least 180,000 people.

VOLTA infostealer uses Claude, Gemini and Kimi to rank victims.

Google adds a $250,000 "root-in-cloud" bug bounty reward.

Russia's statistics agency hit; hacktivists claim it.

What to do before the next shift

Rank by what is reachable and actively attacked, not by CVSS alone.

#	SYSTEM	STATUS	ACTION	CLOSE WITH
1	**Refrigeration supervisors**	Attacked	Pull off the internet; verify defrost settings; VPN-only access	External re-scan, alarm test
2	**Synology NAS**	Attacked	Close 5000/5001 forwards; update to SA-26:13 builds; replace EoL hardware	Build number, offline restore test
3	**CryptoPayment Gateway**	Attempts	Delete plugin files; rotate keys; move funds to fresh wallets	Checksums, payout audit
4	**Node-RED · IoT2050**	Scanned	V4.3.4.1+; adminAuth on every instance; audit exec flows	/flows returns 401
5	**Microsoft 365 / Entra**	Phished	Block device code flow (report-only first)	Policy on, sign-in log review
6	**Langflow**	Public exploit	Upgrade to 1.13.0; remove internet exposure	Version, firewall rule
7	**LXD · MicroCloud · Incus**	Critical, unexploited	Snap refresh; restrict the HTTPS API	snap list output
8	**Third-party page scripts**	Supply chain	SRI hashes, script-src CSP, self-host critical tags	CSP report, tag inventory
9	**Linux and IoT with Telnet**	Botnet	Disable Telnet; no empty root passwords	Port 23 closed

FIRST HOUR

Name an owner for each system above. Record model, build and whether it is reachable from the internet. Anything exposed and attacked gets contained now, coordinated with operations.

SAME DAY

Close the risky paths, patch what can be patched and remove what can't. Log every exception with an owner and a deadline instead of marking it done.

24–72 HOURS

Prove recovery: one isolated restore, one alarm test, one denied login. Review vendor accounts and old port forwards. Keep a baseline export per device.

SCHOOLS AND MSPs

Put cafeteria refrigeration, building controls and NAS backup targets in the same inventory. MSPs: one task and evidence record per client; one client's patch proves nothing about the next.

BEFORE YOU ACT

We could not confirm which CVEs CISA added to its Known Exploited Vulnerabilities catalog between 31 October and 3 November. Check the catalog directly and add any matches to this list.

Evidence you can follow

Vendor and CERT advisories first, then reporting. Numbers match the source lines at the foot of each page. Every entry is a live link in the digital edition. Research closed on 3 November 2026; later advisories may change scope or fixes.

01 CERT-FR · Alert ALE-012, 12–16 Oct
cert.cyber.gouv.fr/alerte/CERTFR-2026-AL…

02 Forklog · French supermarket attacks
forklog.com/en/news/hackers-disrupt-refr…

03 Reuters (Yahoo) · Swedish freezers, 2 Nov
yahoo.com/news/world/articles/temperatur…

04 Al Jazeera · Second wave, 2 Nov
aljazeera.com/news/2026/11/2/freezers-in…

05 RefIndustry · Claroty controller flaws
refindustry.com/news/danfoss-copeland-an…

06 Synology · Ransomware warning, 29 Oct
synology.com/en-us/company/news/article/…

07 Synology · Advisory SA-24:20
synology.com/en-global/security/advisory…

08 Synology · Advisory SA-26:13
synology.com/en-global/security/advisory…

09 Gridinsoft · C3RB3R analysis citing 360
blog.gridinsoft.com/synology-c3rb3r-rans…

10 HKCERT · Synology ransomware alert, 2 Nov
hkcert.org/security-bulletin/security-al…

11 Help Net Security · RISK:STATION
helpnetsecurity.com/2024/11/04/cve-2024-…

12 Siemens ProductCERT · SSA-834709
cert-portal.siemens.com/productcert/html…

13 VulnCheck · Node-RED exploitation, 2 Nov
vulncheck.com/blog/exploitation-targetin…

14 Node-RED · Securing Node-RED
nodered.org/docs/user-guide/runtime/secu…

15 WPScan · CryptoPayment Gateway advisory
wpscan.com/vulnerability/9b1490a0-1381-4…

16 THN · CryptoPayment attempts, 3 Nov
thehackernews.com/2026/11/attackers-targ…

17 THN · Weekly recap, 2 Nov
thehackernews.com/2026/11/weekly-recap-c…

18 Microsoft · Storm-2372 (background)
microsoft.com/en-us/security/blog/2025/0…

19 Microsoft Learn · Block authentication flows
learn.microsoft.com/en-us/entra/identity…

20 The Record · FBI on Binance theft
therecord.media/fbi-blames-tradertraitor…

21 THN · TraderTraitor and Binance
thehackernews.com/2026/11/fbi-links-nort…

22 The Record · Mercado Bitcoin heist
therecord.media/mercado-bitcoin-brazil-c…

23 THN · Polymarket $2.7M theft
thehackernews.com/2026/11/hackers-steal-…

24 The Record · Polymarket refunds
therecord.media/polymarket-returning-fun…

25 SecurityWeek · DebugBear cites DNS hijack
securityweek.com/polymarket-returns-3-9-…

26 Chainalysis · Security incident, 30 Oct
chainalysis.com/blog/security-incident-o…

27 THN · Google disrupts x.cpe botnet
thehackernews.com/2026/11/google-disrupt…

28 THN · LXD and MicroCloud flaw
thehackernews.com/2026/11/critical-lxd-a…

29 THN · Langflow flaws
thehackernews.com/2026/11/critical-langf…

30 SecurityWeek · Ivanti zero-days
securityweek.com/ivanti-patches-two-more…

31 The Record · Apple alerts, 99 countries
therecord.media/apple-warns-users-99-cou…

32 The Record · BYOD gang and Michigan State
therecord.media/michigan-state-universit…

33 THN · VOLTA infostealer (briefs)
thehackernews.com/2026/11/new-volta-info…

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 · 3 November 2026
Understand the threat. Build the defense.