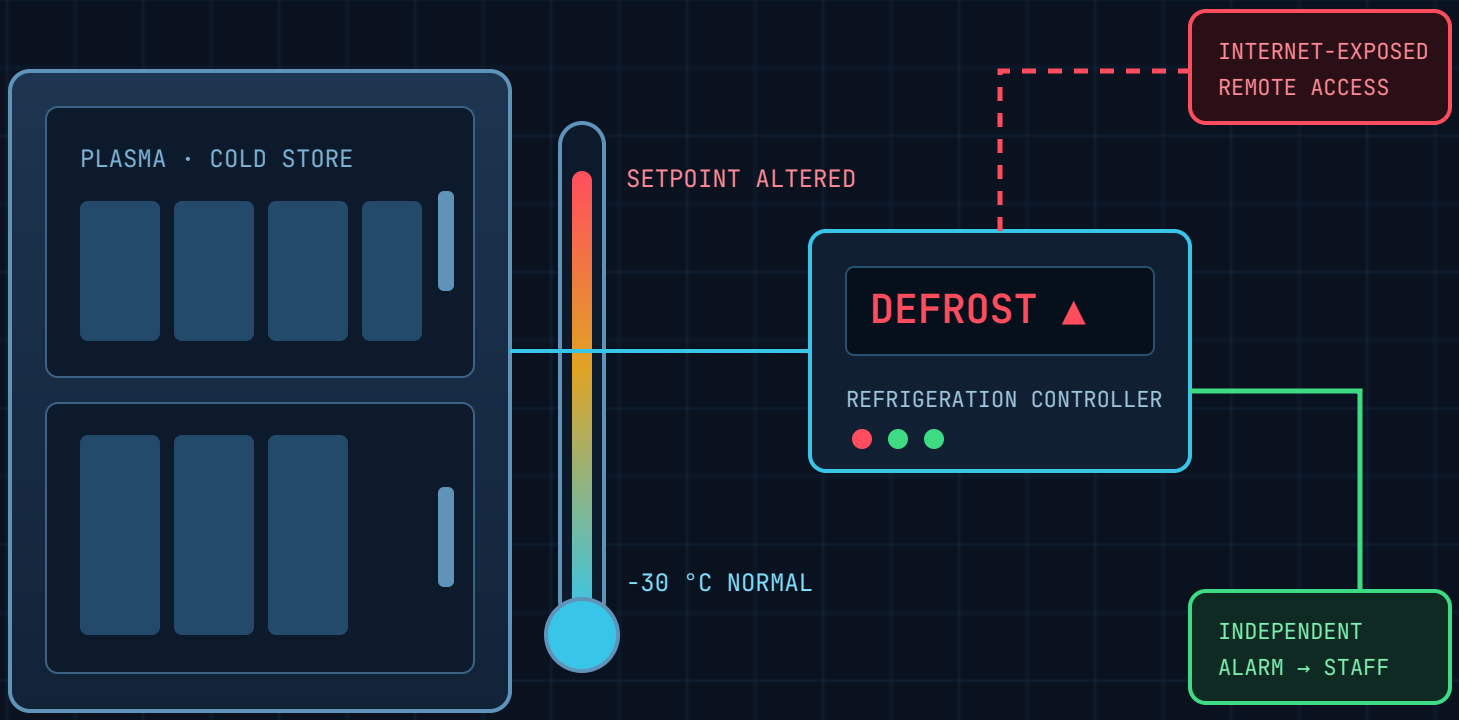
DAILY

FRIDAY · NOVEMBER 06 · 2026

MAG212 CYBER

DAILY CYBER INTELLIGENCE



The cold chain is now a target

US agencies issue joint warning after French plasma stores and European supermarkets see freezer setpoints altered remotely

PATCH NOW
OpenSSH "sshole": Alpine password bypass

DEADLINE TODAY
WordPress CVE-2026-119977 in CISA KEV

ZERO-DAY
Zyxel GS1900 switches: June patch fell short

EXECUTIVE BRIEFING

What matters today

Two flaws moved from “patched” to “exploited” this week, and governments on both sides of the Atlantic warned that attackers are changing freezer setpoints in critical cold storage. Here are the three actions that matter most this shift.

1. **Patch and lock down Alpine / musl SSH now**
   OpenSSH’s password bypass (CVE-2026-123158) was used to get root on a research honeypot; the first attempt came less than nine hours after disclosure. Install your branch’s fixed `openssh` package and restart `sshd`, or set `PasswordAuthentication no` immediately.[12][8]

2. **Confirm every WordPress site is on a fixed release**
   CISA added CVE-2026-119977 to its Known Exploited Vulnerabilities catalog on Nov 3 with a federal deadline of **today**. Fixed in 7.1.4 and back-ported releases down to 4.7.39.[14][13]

3. **Take refrigeration controllers off the internet**
   CISA, FBI, HHS, USDA and DOT urge operators to remove internet exposure, isolate controllers and alert on setpoints outside safe ranges. Check the same for Zyxel GS1900 switch management interfaces.[2][17]

> **How to read this issue.** Each story separates **confirmed facts** (vendor, government or original researcher), **reported claims** (attributed to the outlet that made them) and **MAG212 CYBER analysis**. Diagrams use solid boxes for documented steps, dashed boxes for unknown steps and green boxes for recommended defenses. Numbers in brackets link to the source register on page 16.

IN THIS ISSUE

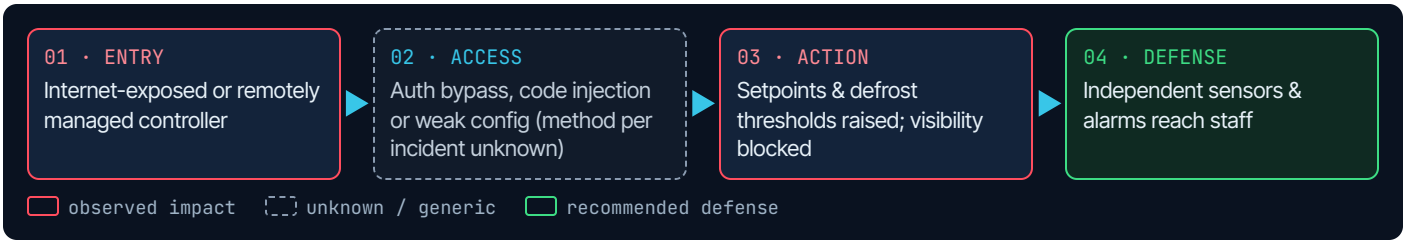
The cold chain under attack 03
OpenSSH “sshole” exploited 05
Field guide: Alpine SSH fix 06
WordPress KEV deadline today 07
Zyxel GS1900 zero-day 08
OFBiz: 46 CVEs in one release 09
DreamHost breach details 10
The phishing kit that fakes its takedown 11
Briefs: ChatGPT & kernel research 12
Defender’s Action Desk 13
Awareness lesson & subscribe 14
Editor’s verification notes 15
Source register 16

01 / CRITICAL INFRASTRUCTURE ACTIVE CAMPAIGN

The cold chain under attack

After weeks of remotely triggered defrost cycles in European supermarkets and an attempt on French plasma stores, five US agencies have told operators to harden refrigeration and cold-chain monitoring systems.

US WARNING	EU WARNING	FRANCE · EFS	CVE / VENDOR
Nov 5 · CISA, FBI, HHS, USDA, DOT	**Nov 4 · Commission, ENISA, Europol**	**3 plasma sites · Mon Nov 2**	**None named in US alert**



Attack pattern as described in reporting on the US alert and the EFS statement. Step 02 is generic: the initial access method for EFS has not been disclosed. Diagram: MAG212 CYBER. [3][4]

What happened

Confirmed (EFS, via Euronews and AP): On Monday, Nov 2, temperature and defrost thresholds were raised "to extremely high levels" at three cold-storage sites of France's blood service, the Établissement français du sang (EFS), through an incident at a refrigeration supplier. Monitoring and alarms detected the anomaly, staff moved or secured plasma for transfusion and medicine manufacturing, and EFS says no blood products were lost and collection continues. [4][5]

Supplier: Coolworld says the incident involves remote-monitoring software for refrigeration, that the vulnerability lies in a component from a third-party vendor, and that a limited number of units were affected. [6]

Reported, not confirmed: Le Canard Enchaîné, which first reported the attack, said attackers tried to push temperatures as high as 110 °C, against a normal −30 °C (as relayed by AP). [5]

Why it matters now

On Nov 5, CISA, the FBI, HHS, USDA and DOT jointly urged critical infrastructure to harden industrial refrigeration and cold-chain monitoring, saying such attacks are occurring worldwide across healthcare, food and agriculture, chemicals and transportation. According to reporting on the alert, it names no manufacturer, cites no CVE and attributes the activity to no group. [3][1] A day earlier, the European Commission, ENISA, Europol and national authorities issued their own call to secure exposed equipment. [2]

Who is affected

Any operator whose refrigeration or temperature controllers, monitoring portals or vendor support tools are reachable from the internet or shared business networks: hospitals and blood services, food retail and distribution, pharmaceutical cold chains and refrigerated transport. No specific product versions are confirmed for the EFS incident.

01 / CRITICAL INFRASTRUCTURE · CONTINUED

Timeline: how the refrigeration campaign unfolded

Date	Event	Status
Late Aug 2026	Freezer malfunctions begin at about six US military commissaries; Pentagon investigating whether they were cyberattacks.[2]	Under investigation; no conclusion
Oct 11 (overnight)	Defrost function triggered remotely at ~300 Intermarché/Netto and fewer than 100 Coopérative U stores in France. BFMTV reported Danfoss controllers on older software.[7]	Confirmed by retailers; vendor link reported, not confirmed by Danfoss
Oct 12	Danfoss says most affected units were older models no longer receiving updates (AK-SM 800, AK-SC 355), AP reported.[5]	Vendor statement
Nov 2 (Mon)	EFS: thresholds raised at three plasma cold-storage sites via supplier incident.[4]	No products lost
Nov 4	EU joint warning (Commission, ENISA, Europol, national authorities).[2]	Issued
Nov 5	US joint guidance from CISA, FBI, HHS, USDA, DOT.[3]	Issued

No public source links these incidents to a single actor. Treat them as a pattern of targeting, not a proven single campaign.

How the attack works

Reporting on the US alert describes attackers exploiting unpatched or internet-exposed controllers through authentication bypass, code injection or weak configuration, then forcing continuous heating or defrost cycles and, in some cases, blocking operators from seeing current temperatures.[3] For EFS, initial access, credential use and persistence are not public.

What defenders should look for

- Setpoint or defrost-threshold changes outside approved ranges, especially overnight.
- Logins or vendor-support sessions from unfamiliar IP addresses.
- Controller readings that disagree with independent sensors.
- Controllers or monitoring portals visible on the public internet.

Maintenance, sensor faults and authorized defrost schedules can explain some changes. Confirm with the site team before escalating.

How to investigate

Preserve controller, gateway and monitoring logs with the facility team. Line up setpoint history, operator identities, remote-session records and measured temperatures on one timeline. Have quality assurance assess product integrity separately from the cyber investigation.

Contain and remediate

Follow safety procedures first: move product, then investigate. The US guidance, as reported, recommends:[3]

- Remove controllers from the internet; put any needed remote access behind a firewall or patched edge device.
- Isolate OT on a dedicated VLAN, apart from business networks.
- Replace default passwords; use phishing-resistant MFA where possible.
- Update firmware; plan to retire end-of-support equipment.
- Allowlist the devices and IPs that may change configuration.
- Keep tested offline backups and enable logging.
- Define safe setpoint ranges and alert when they are exceeded.

Verify recovery

Confirm approved setpoints on every unit, prove alarms reach on-call staff without relying on the vendor channel, and get quality sign-off before returning storage to service.

Prevention

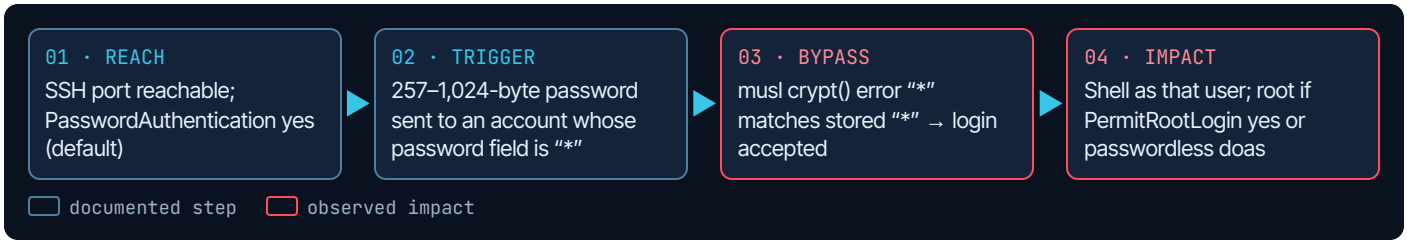
MAG212 analysis: The EFS outcome shows the value of an alarm path the attacker does not control. Ask suppliers who can change setpoints remotely, how that access is logged, and how fast you are told.

02 / REMOTE ACCESS EXPLOITED

OpenSSH “sshole”: patch Alpine now

A password bypass on musl-based Linux without PAM was used to get root on a research honeypot, with the first attempt less than nine hours after disclosure. If you run Alpine with password logins enabled, act now.

CVE	FIXED	AFFECTS	EXPLOITATION
CVE-2026-123158	OpenSSH 10.6p2 · Nov 5	OpenSSH ≥7.3p1 · musl · no PAM	Honeypot root · Nov 5–6



Failure path as documented by Alpine Linux and Wakefield. Also requires at least one other local account with a SHA-256 or SHA-512 (5/6) hash. Diagram: MAG212 CYBER.[8][10]

Exploited (honeypot) · Public PoC · Patch available · Not in CISA KEV as of cutoff

What happened

OpenSSH 10.6p2 shipped on Nov 5 with a “critical security workaround” for a password-authentication bypass on Linux systems using musl libc with PAM disabled. The issue was reported by Özgün Kültekin of Wakefield, and Alpine published fixed packages for every supported branch the same day.[9][8] Hong Kong’s GovCERT tracks it as CVE-2026-123158 and notes public proof-of-concept code.[11]

Exploitation: Previdian reports eight attempts from one Japan-based IP address and confirmed “successful root access” on an Alpine honeypot; the first attempt came less than nine hours after the CVE was published. The attacker ran reconnaissance (`id`, `uname`, `hostname`). This is a single source: no production compromises have been reported, and Orca and Safe Security said exploitation in the wild had not been established.[12]

Who is affected

Alpine’s standard `openssh-server` package, or `openssh-server-pam` with `UsePAM no`, when password logins are enabled and a key-only account (password field “*”) exists.[8] SOCRadar flags Alpine tiny-cloud AWS and Azure images 3.18.11–3.24.3, whose default user has passwordless `doas`. The researcher also flags OpenWrt, Buildroot, Yocto and some Docker images. glibc systems, PAM-enabled builds, Dropbear and OpenBSD are not affected.[12]

What to look for

“Accepted password for” lines in `/var/log/messages` for accounts that have no password, such as `alpine`, `root` or any key-only user. Review `doas` use, new users, new files and new `authorized_keys` entries. If a login cannot be ruled out, Alpine says to treat the machine as compromised.[8]

Contain and remediate

Restrict SSH reachability first. Install your branch’s fixed package (table, page 6), then run `rc-service sshd restart`: upgrading alone does not replace the running daemon. If you cannot update, set `PasswordAuthentication no` and restart, keeping a working key session open. OpenSSH’s Damien Miller told admins of affected systems to do this “IMMEDIATELY.”[12] Previdian warns that public exploit code is unverified and may contain malware: do not run it.

Verify recovery

Record the installed package and sshd restart time, confirm `sshd -T` shows the intended settings, and test a fresh key-based login before closing your session.

FIELD GUIDE / ALPINE LINUX

Check, fix and prove the SSH patch

Alpine back-ports the fix into each stable branch, so compare the full package revision for your branch rather than the upstream version number.

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

Source: Alpine Linux advisory, Nov 5, 2026.[8] Versions copied verbatim. Releases older than 3.16 are not listed: move them to a supported branch.

READ-ONLY · Alpine · ash · apk · any user

```
# 1. Which openssh build is installed?
apk list --installed 'openssh*'

# 2. What does the running config allow? (root)
sshd -T | grep -Ei '^(passwordauthentication|usepam|permitrootlogin) '

# 3. Any password logins to key-only accounts? (root)
grep 'Accepted password for' /var/log/messages
```

Purpose: compare the installed revision with the table, confirm effective settings, and look for suspicious password logins. `sshd -T` prints the effective configuration and needs to read host keys; add `-C user=…,host=…,addr=…` to evaluate Match blocks.[27] Log path applies where syslog writes to `/var/log/messages`, as Alpine's advisory assumes. Syntax checked against documentation; not executed on an Alpine host for this issue.

CHANGES SYSTEM · Alpine · ash · root

```
# Update and restart (keep your current session open)
apk upgrade openssh
rc-service sshd restart
```

From the Alpine and Wakefield guidance. The restart is required: the running daemon keeps the old binary until restarted.[8][10] Confirm key login from a second terminal before closing the first. Not executed for this issue.



Recommended workflow. MAG212 CYBER.

03 / WEB PLATFORMS CISA KEV · DUE TODAY

WordPress: the upgrade window is the attack window

A race condition in WordPress core lets an unauthenticated attacker run code during a full core upgrade. CISA confirmed exploitation, and US federal agencies must be patched by today.

CVE	FIXED	SEVERITY	KEV
CVE-2026-119977	7.1.4 (Oct 28) + back-ports	CVSS 8.1 (Wordfence)	Added Nov 3 · due Nov 6



Time-of-check/time-of-use race (CWE-367) as described by CISA and Wordfence via The Hacker News. Diagram: MAG212 CYBER.[14]

What happened

WordPress 7.1.4, released Oct 28, fixed "a weakness in the WordPress upgrade process which can lead to remote code execution during the upgrade window," credited to Umut Bayram, alongside a dozen stored-XSS and disclosure fixes.[13] CISA added the flaw to KEV on Nov 3, setting a Nov 6 deadline for federal civilian agencies.[14]

Activity: Wordfence recorded more than 18,500 requests targeting staged installer paths in the first 21 hours after disclosure. Previdian's honeypots logged three attempts on Oct 30.[14] Attempts are not proof of successful compromise.

Who is affected

WordPress 4.7.0 through 7.1.3 on unpatched branches. Wordfence rates it CVSS 8.1; WordPress's own advisory rates it Low, reflecting the narrow timing window.[16][15] Versions 4.6 and earlier receive no fixes.

What to look for

Web requests to upgrade staging or installer files around the time an update ran, unexplained new PHP files, changed core files, unknown administrators and unusual outbound connections. Line these up with your update start and end times.

Contain and remediate

Update to the fixed release for your branch (table below). If a site updated while exposed, preserve logs, then run a checksum verification and review plugins, themes and uploads, which checksums do not cover.

Verify recovery

Record the core version and a clean checksum result for each site, and confirm auto-updates stay enabled.

Branch	Fixed	Branch	Fixed	Branch	Fixed	Branch	Fixed
7.1	7.1.4	6.7	6.7.11	6.3	6.3.14	5.9	5.9.20
7.0	7.0.8	6.6	6.6.11	6.2	6.2.15	5.8–5.0	see [16]
6.9	6.9.11	6.5	6.5.14	6.1	6.1.16	4.9	4.9.35
6.8	6.8.12	6.4	6.4.14	6.0	6.0.18	4.7	4.7.39

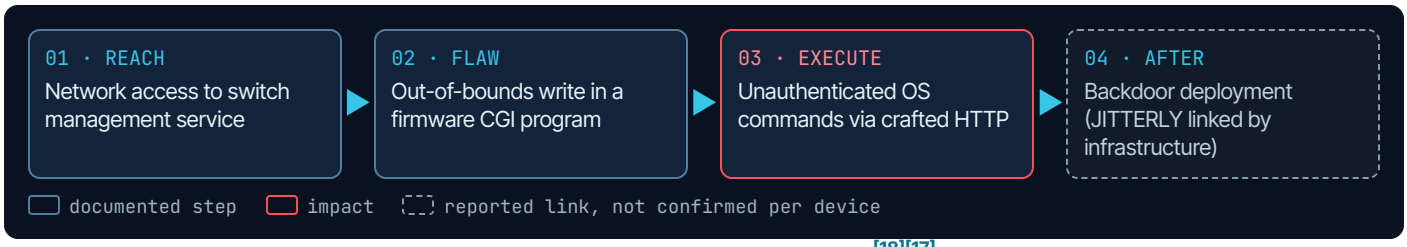
Branch table compiled by AICybr from WordPress release data; wordpress.org confirms back-ports "through 4.7." Verify your exact build on wordpress.org.[16][13]

04 / NETWORK EDGE ZERO-DAY (RESEARCHER)

Zyxel GS1900: the patch that didn't stop the attack

Attacks on nearly 1,000 Zyxel switches were blamed on a flaw fixed in June. Binarly says the attackers had moved to a new, unpatched bug. Zyxel has now shipped "Patch 3."

NEW CVE	SEVERITY	AFFECTS	FIX
CVE-2026-107441	8.8 Zyxel · 9.8 Binarly	10 GS1900 models ≤ Patch 2	Patch 3 firmware



Based on ThaiCERT and The Hacker News reporting of Binarly's research. Diagram: MAG212 CYBER.[18][17]

Exploitation: researcher assessment | Patch available | Not in KEV as of Nov 5 report

What happened

GreyNoise reported that attackers took data from 996 GS1900 switches around Aug 17, tied at the time to CVE-2026-7273 (fixed in "Patch 2," June 16; added to KEV Sept 21). Of those, 564 still used factory-default credentials.[17] On Sept 17 Binarly found an exploit on a server that also acted as a command server for the JITTERLY backdoor, determined that it worked against Patch 2, and reported it to Zyxel on Sept 29.[17] ThaiCERT warned on Nov 6.[18]

Uncertainty: Zyxel's advisory does not say whether CVE-2026-107441 was exploited, and neither researcher says whether the compromised switches ran Patch 2. Attribution to a group Acronis tracks as Red Heron is tentative.[17]

Who is affected

GS1900-8, -8HP, -10HP, -16, -24, -24E, -24EP, -24HPv2, -48 and -48HPv2 on Patch 2 or earlier. Example fixed builds: `2.90(AAHH.3)C0` for GS1900-8 and `2.90(AAHL.3)C0` for GS1900-24; check Zyxel's advisory for your model.[17]

What to look for

Management access from unexpected hosts, configuration or account changes, unexpected reboots and outbound connections from switch management IPs. Zyxel has published no compromise indicators.

Contain and remediate

Install Patch 3 firmware. Zyxel lists no workaround. **MAG212 analysis:** until patched, allow management only from a dedicated admin network, replace default credentials, and treat any switch with signs of tampering as untrusted: back up its configuration for evidence, then reflash from Zyxel firmware and rebuild credentials.

Verify recovery

Confirm the firmware build shown in each switch's web interface (labels vary by model), and test that management is unreachable from user VLANs.

05 / ENTERPRISE APPLICATIONS PATCH NOW

Apache OFBiz fixes 46 CVEs in one release

Version 24.09.08 closes several unauthenticated remote-code-execution paths, a hard-coded JWT key and dozens of authorization gaps in the open-source ERP and e-commerce suite.

ANNOUNCED	CVES	AFFECTED	EXPLOITATION
Nov 4 · oss-security	46	All before 24.09.08	None reported

CVE	Title (as announced)	Access
CVE-2026-68524	Pre-Authentication Remote Code Execution via Attacker-Controlled Screen Definition Loading	Unauthenticated
CVE-2026-73578	Unauthenticated saved-view authorization bypass with RCE impact	Unauthenticated
CVE-2026-83542	Unauthenticated RCE via login-page widget injection	Unauthenticated
CVE-2026-105330	Use of Hard-coded Cryptographic Key in JWT Token Authentication Enables Unauthenticated Administrative Access	Unauthenticated
CVE-2026-92887	REST API authentication bypassed by default when the auth attribute is omitted	Unauthenticated
CVE-2026-109928	Incorrect Authentication Algorithm in Password Reset Enables Full Account Takeover	Unauthenticated
CVE-2026-81815	SQL injection – performFind ignore-case values, MySQL/MariaDB	See advisory

Seven of the 46 CVEs, titles quoted from the Apache announcement; access level inferred from each title. The announcement gives no CVSS scores and says the set includes “some critical issues.”[19][20]

What happened

On Nov 4 the OFBiz project announced 46 CVEs affecting all versions before 24.09.08 and advised users to upgrade.[19] We found no report of exploitation; OFBiz flaws have been exploited quickly in past years, so treat internet-facing instances as urgent.

How it works

Several paths let untrusted request input choose screens, views, widgets or expressions that the server then renders or executes. Code runs with the application’s privileges. Details of each path are in the linked fixes.

What to look for

Unauthenticated requests to manager routes, rendering errors, unexpected JWTs accepted by the API, new admin users, Java child processes and new outbound connections. One error alone proves little.

Contain and remediate

Restrict management routes to trusted networks, preserve logs and snapshots, then deploy 24.09.08. Because CVE-2026-105330 involves a hard-coded JWT key, rotate secrets and review admin sessions after upgrading. Where code execution is plausible, rebuild from a trusted artifact.

Verify recovery

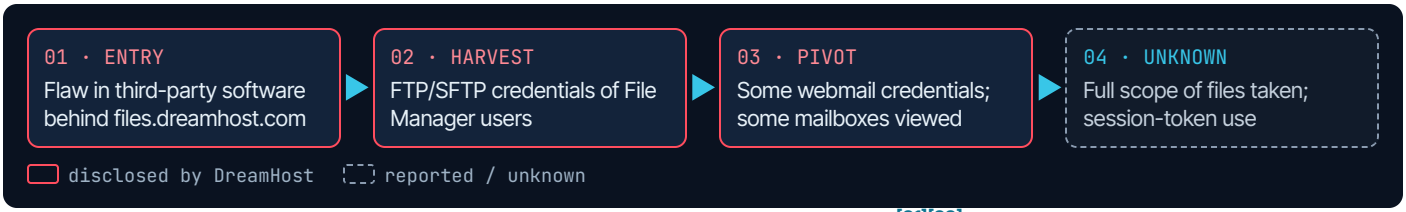
Confirm 24.09.08 on every node (including staging and standby), test that protected views reject anonymous requests, and smoke-test manager workflows.

06 / HOSTING UPDATE

DreamHost: two months inside the file manager

The hosting provider says a third-party flaw in its web-based File Manager exposed FTP/SFTP and some webmail credentials for users who logged in between about August and Oct 23.

DETECTED	EXPOSURE WINDOW	SCOPE	CVE
Oct 23, 2026	~Aug → Oct 23	"Well under 10%" of accounts	None disclosed



Based on DreamHost's Oct 29 disclosure and TechCrunch's Nov 4 reporting. Diagram: MAG212 CYBER.[21][22]

What happened

Confirmed (DreamHost): Unauthorized access to the server running File Manager was discovered on Oct 23. The attacker obtained FTP/SFTP usernames and passwords of users who logged into File Manager between approximately August and Oct 23, credentials for a limited number of webmail users, and in a small number of cases may have viewed mailbox contents. DreamHost found no evidence of access to control-panel logins or billing data.[21]

Reported: TechCrunch, citing DreamHost's California data-breach notice, says the attack began in August and that session tokens and customer files were taken. DreamHost declined to explain the detection delay.[22]

Who is affected

DreamHost says "well under" 10% of email and FTP/SFTP accounts; it touts about 400,000 paying customers but gave no exact figure. Use DreamHost's direct notice to confirm your own exposure.

What DreamHost did

Took File Manager offline, fixed the flaw, reset exposed passwords and ended sessions, rotated internal credentials, rebuilt the tool with added monitoring and began notifying regulators.[21]

What customers should check

- Site files changed since August: compare with a known-good copy.
- New mailbox forwarding rules, filters or app passwords.
- New FTP/SFTP users and unknown WordPress admins.
- Secrets stored in hosted files (API keys, database passwords): rotate them.

Verify recovery

Confirm resets through the official panel, review mail routing and admin lists, and watch downstream services for use of retired secrets.

Prevention

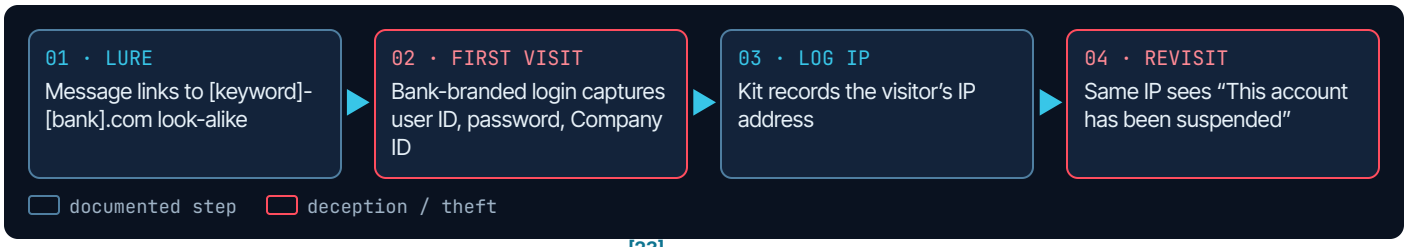
Use unique credentials per service, prefer SFTP keys over passwords, and keep deployment secrets out of the web root.

07 / FRAUD & IDENTITY LIVE CAMPAIGN

The bank phishing kit that fakes its own takedown

KELA mapped look-alike sites for 189 US financial institutions that show a fake “account suspended” page to anyone who checks twice, fooling scanners and takedown teams.

BANKS IMPERSONATED	RESEARCH	FRONTING	CVE
189 (183 live Oct 25)	KELA · updated Nov 3	Cloudflare + shared hosting	Not applicable



Conditional delivery as documented by KELA. Diagram: MAG212 CYBER.[23]

What happened

KELA documented infrastructure impersonating 189 US banks and credit unions; 183 still had live look-alike domains on Oct 25. The same back end also served lures for UK, Dutch, Australian and New Zealand brands. KELA traced operator activity to a UK residential connection and calls it a lead, not an identification.[23]

How it works

A first visit from an IP gets the fake login. A repeat visit from the same IP gets a fake hosting “suspended” notice, a block page, a blank page or a redirect to Google. Domains sit behind Cloudflare, with origins on shared cPanel hosting alongside hundreds of unrelated sites.[23]

What to look for

Domains following `[secure|protect|authorize|cancel…]-[bank].com`, business-banking lures (“treasury-portal,” “help-desk”), a tab title copying Cloudflare’s “Attention required” page, and credential POSTs to the same domain. Examples KELA names include `53primaryset[.]com` and `authorize-valley[.]com`.

How to investigate

Preserve the original message and the first response if captured. Re-check from fresh IP addresses over several days, avoiding anonymizing networks the kit blocks. Never enter real credentials.

Contain and remediate

Block confirmed domains (not the shared origin IPs, which host unrelated sites). Report to the bank, registrar, Cloudflare and host. If anyone entered credentials, call the bank on its known number, reset passwords and review recent transfers.

Prevention

Business banking users should reach the bank only from a saved bookmark or its app, and confirm transfer-related requests by phone.

08 / AI SECURITY

A ChatGPT preview feature slipped past Lockdown Mode

Fixed by OpenAI (Sept 18) | No real-world abuse reported

What happened: Check Point Research disclosed on Nov 5 that HTML previews in ChatGPT code blocks, rendered in nested sandboxed frames, still allowed popups to escape. A new nested frame gave access to an unmodified popup function, bypassing Lockdown Mode.[24]

Impact demonstrated: A malicious GPT silently leaked chat messages to an attacker server. In the Electron desktop app this needed no click. A fake-update lure still required the victim to click a download link, and researchers could force a sign-out and redirect to an attacker login page.[24]

Status: OpenAI told the researchers on Sept 18 it had removed the sandbox permissions involved; Check Point confirmed the technique no longer works. No CVE.

Takeaway: Keep managed desktop clients current, treat third-party GPTs as untrusted input, and don't rely on a single product setting to protect sensitive data.

09 / SECURITY RESEARCH

AI agents found 1,169 Linux root exploits



Research pipeline, not an intrusion chain. Figures as reported by SecurityWeek from OpenAI's Nov 4 post; OpenAI's page could not be retrieved for this issue.[25][26]

What happened: OpenAI ran an autonomous pipeline with an unreleased cyber model against the Linux kernel master branch in mid-October, at about $1.21M in API credits. It reports hundreds of reports and patches submitted upstream; more than 100 local privilege escalations were patched or had staged patches within 10 days.[25]

What it does not mean: These are not 948 new CVEs, not a per-distribution exposure list, and not evidence of attacks. They are local escalations: an attacker needs code running on the machine first.

What to do: Map your running kernels to your distribution's advisories as fixes land, prioritize shared and multi-tenant hosts, and keep the patch-and-reboot cycle short. Use `uname -r` to record the running kernel (page 13).

DEFENDER'S ACTION DESK

Today's checklist

#	Action	Owner	Proof to close the ticket
1	Patch or disable password auth on musl/Alpine SSH	Infra / cloud	Fixed package, sshd restart time, `sshd -T` output, log review
2	Update every WordPress site to a fixed release	Web / MSP	`wp core version` + clean `verify-checksums`
3	Remove internet exposure of refrigeration / BMS controllers	Facilities + IT	External scan clean; setpoint alerts tested
4	Flash Zyxel GS1900 to Patch 3; restrict management	Network	Firmware build per switch; ACL test from user VLAN
5	Upgrade OFBiz to 24.09.08; rotate secrets	App owner	Build on all nodes; anonymous access test
6	DreamHost customers: review mail rules & site files	Site owner	Rules audit; file diff vs known-good

READ-ONLY · Linux · bash · WP-CLI · site file owner

```
# Run in the WordPress root as the user that owns the files
wp core version
wp core verify-checksums
```

Prints the installed core version and compares core files with WordPress.org checksums. Checksums do not cover plugins, themes or uploads. Requires WP-CLI. Syntax checked against WP-CLI documentation; not executed against a live site for this issue.[28]

READ-ONLY · Linux · POSIX shell · uname · any user

```
uname -r
```

Prints the running kernel release. Run on the actual host or node, not inside a container image. Compare with your distribution's advisory; the string alone doesn't show which back-ports are installed.[29]

First hour: establish scope

Record asset, owner, exact running build, exposure path and time checked. MSPs: keep a per-tenant list. Schools: test the management boundary from staff, student and guest VLANs with authorized accounts.

Same shift: protect evidence

Export firewall, reverse-proxy, endpoint and identity logs before rebooting or reflashing. Note clock offsets and retention gaps.

Close the ticket: verify independently

A patch closes the door but doesn't prove no one came in. Require a running-version record, an exposure check from the right network and a service smoke test. Escalate if execution or credential abuse is suspected.

Escalate: one owner

Name one incident lead, separate observed events from hypotheses, and record timestamps and patch provenance.

TWO-MINUTE LESSON · FOR STAFF AND BUSINESS LEADERS

"Your account is suspended" is not proof

A text says your business bank account is locked. You open the link, log in and nothing happens. Later IT opens the same link and sees "This account has been suspended." Case closed? No.

What is going on

Modern phishing kits show different pages to different visitors. The first visit steals your login; later visits show a decoy so investigators think the site is already gone.[23]

Do this every time

- Open your bank only from a saved bookmark or its app.
- Verify payment or account changes by calling the number on your card or contract.
- Report suspicious messages even if the link now looks dead.

If you already entered details

Call the bank on its official number, tell IT the time, message and device, keep the message, and follow the bank's instructions to secure the account.

For leaders: the cold-chain lesson

Ask three questions about anything that keeps products, medicine or data safe: who can change it remotely, would we know within minutes, and does our alarm still work if the vendor's system is compromised? EFS kept its plasma because the answer to the last one was yes.[4]

Watch list. Microsoft's November Patch Tuesday is Nov 10. Expect follow-up on OpenSSH exploitation, a possible CISA KEV listing, and more refrigeration-sector guidance from European CERTs.

MAG212 CYBER lands in your inbox, free

Daily intelligence, new magazine editions, threat alerts and practical cheat sheets for IT teams, MSPs and business owners. No cost, unsubscribe anytime.

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

EDITORIAL TRANSPARENCY

How we checked this issue

Every story was re-checked against vendor, government or original-researcher sources before publication. Where we could not reach a primary page, we say so.

Story	Primary sources checked	Open questions
Cold chain	Euronews & AP (EFS statement), Coolworld, The Record, Defense One, IT-Connect	CISA and EFS pages blocked our fetcher; their content is taken from outlets that link to them. Initial access for EFS not disclosed. No attribution.
OpenSSH	Alpine advisory, OpenSSH release notes, Wakefield, GovCERT.HK, Help Net Security	Exploitation seen on one honeypot only. Not in KEV at cutoff.
WordPress	wordpress.org 7.1.4 post, The Hacker News (CISA/Wordfence), WordPress GHSA	Back-port table is compiled by a third party; confirm per branch on wordpress.org. No confirmed successful compromise in cited data.
Zyxel	The Hacker News, ThaiCERT	Zyxel does not confirm exploitation of CVE-2026-107441. Attribution tentative.
OFBiz	Apache announcement (oss-security), OFBiz security page	No CVSS scores published.
DreamHost	DreamHost disclosure, TechCrunch	File theft and session tokens rest on TechCrunch's reading of the filing.
KELA	KELA research blog	Operator not identified.
ChatGPT	Check Point Research	No independent confirmation; fixed.
Kernel research	SecurityWeek	OpenAI's own post could not be retrieved.

Changes from the earlier draft of today's issue

- **OpenSSH:** now reported exploited against a honeypot; draft said exploitation was not established.
- **Corrected Nov 6, 1 PM PST:** "nine hours" refers to the first attempt, not to root access; the Ahold Delhaize sales figure was removed because reporting ties it to a separate IT incident.
- **Cold chain:** added the Nov 5 US joint guidance, the Nov 4 EU warning and the October retail attacks; promoted to lead.
- **Kernel research:** 1,169 exploits and 948 patches; draft labelled 948 as "unique LPEs."
- **Added:** WordPress CVE-2026-119977 (KEV deadline today) and Zyxel GS1900 CVE-2026-107441.
- **Precision:** OFBiz scope (46 CVEs), KELA count (189), DreamHost exposure window, Check Point fix date. Unverified California filing date removed.

Visuals and commands. All diagrams are MAG212 CYBER explanatory graphics; the cover is a conceptual illustration. No screenshots in this issue. Commands were checked against official documentation but were not executed on affected systems; any output you see will be your own.

EDITORIAL REGISTER

Sources

01 CISA · US partners urge hardening of industrial refrigeration and cold-chain monitoring (Nov 5)
02 Defense One / Nextgov · US agencies warn of refrigerator hacks (Nov 5)
03 IT-Connect · FBI and CISA warn of refrigeration attacks (Nov 5)
04 Euronews · Cyberattack hits French blood banks (Nov 4)
05 CBS News / AP · Blood banks hit by cyberattack in France (Nov 4)
06 Coolworld · Cybersecurity update
07 The Record · Cyberattack disrupts refrigeration in France (Oct 11)
08 Alpine Linux · OpenSSH password authentication bypass (Nov 5)
09 OpenSSH · Release notes, 10.6p2 (Nov 5)
10 Wakefield · OpenSSH musl authentication bypass
11 GovCERT.HK · Alert A26-11-09 (Nov 6)
12 Help Net Security · OpenSSH flaw exploited hours after disclosure (Nov 6)
13 WordPress.org · WordPress 7.1.4 (Oct 28)
14 The Hacker News · CISA confirms WordPress core exploitation (Nov 4)
15 WordPress · GitHub advisory GHSA-4w3m-c66w-69mg
16 AICybr · CVE-2026-119977 fixed versions by branch
17 The Hacker News · Zyxel GS1900 patch fails to block zero-day (Nov 5)
18 ThaiCERT · Zyxel GS1900 CVE-2026-107441 (Nov 6)
19 oss-security · Apache OFBiz CVE announcements (Nov 4)
20 Apache OFBiz · Security page
21 DreamHost · October security incident (Oct 29)
22 TechCrunch · DreamHost customer files and inboxes stolen (Nov 4)
23 KELA · Bank phishing campaign with fake takedown (updated Nov 3)
24 Check Point Research · ChatGPT Lockdown Mode bypass (Nov 5)
25 SecurityWeek · AI agents got root via 948 kernel flaws (Nov 5)
26 OpenAI · A thousand fewer paths to root (not retrieved)
27 OpenBSD manual · sshd(8)
28 WP-CLI · wp core verify-checksums
29 Linux man-pages · uname(1)

MAG212 CYBER · Daily Cyber Intelligence · November 6, 2026. Written and edited by El Mostafa Ouchen. Research cutoff 06:10 PST (America/Los_Angeles). Summaries and analysis are original; quotations are attributed. Corrections: cyber.mag212.com/contact. Free subscription: cyber.mag212.com/subscribe-free.