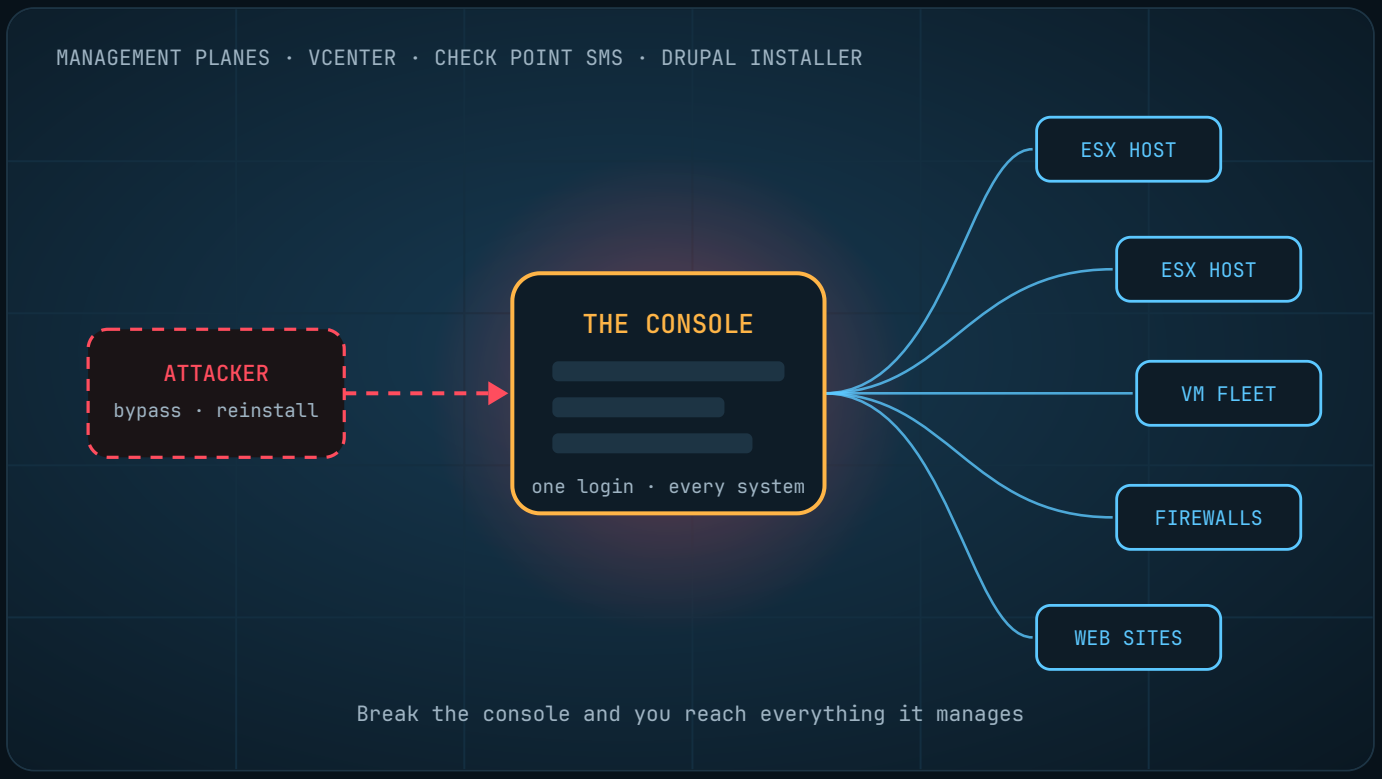
MAG212
CYBER

DAILY

Wednesday, 25 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 7:00 AM PT



VMWARE · CHECK POINT · DRUPAL · MANAGEMENT PLANES

Own the console, own the network

VMware fixed a critical vCenter login bypass and ESX flaws. GreyNoise tracked an attacker running tasks on 24 Check Point firewall managers. Attackers are reinstalling unpatched Drupal sites through their own installer.

03 VMware's 23-bug patch day
04 Patching vCenter and ESX, in order
05 Firewall managers raided, AI suspected
06 Drupal installer exploited
07 Volant Manticore's IPFS backdoor
08 EU Commission, CIA, myColorado
09 Patch board and KEV deadlines

9.8
vCenter auth bypass, ESX RCE

24
Check Point managers used by GT13

27 NOV
KEV due: Drupal, Optimizely

8.0 U3m
vCenter 8 fix; 9.x builds too

What matters today

Published or updated 23–25 November. Theme: the consoles that run everything else.

Virtualisation's keys

Broadcom's VMSA-2026-0011 fixes 23 bugs, including a vCenter login bypass and two ESX remote-code flaws (CVSS 9.8). No exploitation is reported yet. [1]

Firewall managers turned against their owners

GreyNoise watched an actor it calls GT13 run tasks on 24 Check Point management servers at 22+ organisations, copying firewall databases and CA files. [2]

A website's own installer

Drupal's installer can be abused to reinstall and take over a site. Exploited since 19 November; CISA's deadline is 27 November. [4][5]

Patient, quiet espionage

Check Point Research names Volant Manticore, an Iran-linked group hiding commands in IPFS files and posing as job seekers. [6]

THE THREE PRIORITY ACTIONS

1. **Patch vCenter, then ESX.**
   vCenter 9.1.2, 9.0.2.0300 or 8.0 U3m; ESX builds per VMSA-2026-0011. Keep vCenter off the internet. [1]
2. **Update Drupal to 10.6.22, 11.3.22 or 11.4.13, or lock the installer now.**
   Then check for unexpected reinstall activity since 19 November. [4]
3. **Audit Check Point management servers.**
   Confirm the CVE-2026-16232 fix; review management tasks, certificates and /etc/ld.so.preload. [2]

STATUS AT A GLANCE

ISSUE	STATUS	FIX
VMware VMSA-2026-0011	CRITICAL · NOT EXPLOITED	vCenter 8.0 U3m / 9.x
Drupal CVE-2026-132165	EXPLOITED · KEV	10.6.22 / 11.3.22 / 11.4.13
Check Point CVE-2026-16232	USED BY GT13	July 2026 fix
Optimizely CVE-2026-132224	EXPLOITED · KEV	vendor-side; check alerts

CONTENTS

03 VMware VMSA-2026-0011
04 vCenter and ESX patch plan
05 Check Point managers (GT13)
06 Drupal SA-CORE-2026-017
07 Volant Manticore and KuboShell
08 Public sector and breaches
09 Patch board
10 Briefs
11 Defender's Action Desk
12 Awareness: the 'legal' call
13 Sources

BROADCOM VMSA-2026-0011 · 23 CVEs · 24 NOVEMBER

VMware's 23-bug patch day: the four that matter first

A login bypass in vCenter and two remote-code flaws in ESX each score 9.8. Broadcom reports no attacks yet, but vCenter was hit by a similar bug last week.

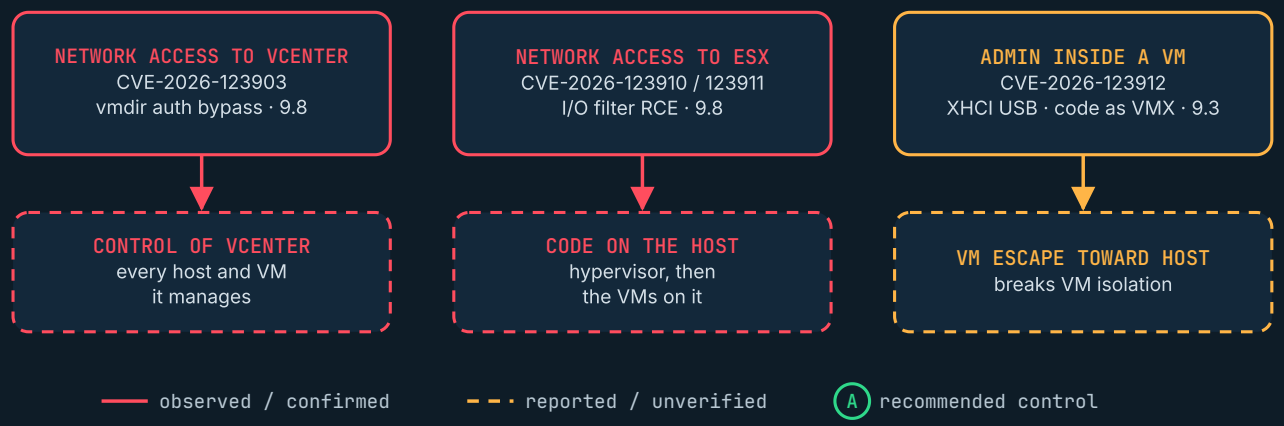


Figure 1 · The three critical paths in Broadcom's advisory. Dashed boxes show what each flaw could lead to; no exploitation has been reported [1]. MAG212 CYBER diagram.

WHAT HAPPENED

On 24 November Broadcom published VMSA-2026-0011, rated critical, covering 23 CVEs across ESX, vCenter, Workstation, Fusion, VMware Tools, Cloud Foundation, Telco Cloud and the Avi Load Balancer. The issues were reported privately. There is no workaround except KB463535 for two ESX 8.0 flaws. [1]

WHY IT IS URGENT

CVE-2026-123903 is in the same directory service (vmdir) as CVE-2026-123890, the separate vCenter bypass CISA listed as exploited on 20 November. Attackers already know where to look. (MAG212 analysis) [1][5]

> **STATUS** Critical. No exploitation reported by Broadcom on 24 Nov. Not in KEV.

THE HEADLINE CVEs

CVE	WHAT	CVSS
CVE-2026-123903	vCenter auth bypass (VMware Directory Service)	9.8
CVE-2026-123910	ESX heap out-of-bounds write, I/O filter service	9.8
CVE-2026-123911	ESX use-after-free, I/O filter service	9.8
CVE-2026-123912	XHCI USB out-of-bounds write (ESX, Workstation, Fusion)	9.3
CVE-2026-123913	ESX VMkernel stack buffer overflow	8.2
CVE-2026-123904-08	vCenter file write, vmdir DoS, local privilege escalation	6.7–7.5

Telco Cloud Platform: KB463501. From VMSA-2026-0011 [1]. Avi Load Balancer and VMware Tools fixes are listed in the advisory.

Patching vCenter and ESX, in the right order

vCenter first: it is the single login that controls every host. Then hosts, then desktop products and Tools.

FIXED VERSIONS

PRODUCT	FIXED IN
vCenter 9.1.x (VCF/VSF)	9.1.2
vCenter 9.0.x (VCF/VSF)	9.0.2.0300
vCenter 8.0	8.0 U3m
VCF vCenter / ESX 5.x	5.2.5
ESX 9.1.x	ESXi-9.1.2.0-25946735
ESX 9.0.x	ESXi-9.0.2.0200-25953133 *
ESX 8.0	ESXi80U3m-25926933
vCenter / ESX 7.0	contact Broadcom (extended support)
Workstation / Fusion 25H2	26H1u1

* On ESX 9.0, CVE-2026-123914 and -123915 are still “Patch Pending”. Telco Cloud Platform: KB463501. From VMSA-2026-0011 [1].

1 · CONTAIN BEFORE YOU PATCH

1. Make sure vCenter and ESX management interfaces are reachable only from an admin network or jump host.
2. If vCenter is internet-facing, take it off now.
3. Snapshot or back up the vCenter appliance before upgrading.

2 · PATCH ORDER

1. vCenter (CVE-2026-123903).
2. ESX hosts, cluster by cluster, with vMotion.
3. Workstation, Fusion and VMware Tools.
4. Avi Load Balancer, if used.

ESX shell (SSH) | root | READ-ONLY

NOT TESTED BY MAG212

check builds

```
vmware -vl
esxcli system version get
```

Shows the ESX build; compare it with the table. On vCenter, check the appliance management interface (port 5480). Not tested by MAG212.

3 · LOOK BACK

- Review vCenter logins, new SSO users, roles and SSH enabled on hosts.
- Check for unexpected VMs, snapshots or exported disks.
- Why: CVE-2026-123890, the earlier vmdir bypass, was exploited before a fix [5].

HOW TO KNOW YOU ARE DONE

Every vCenter and host reports a fixed build; management is reachable only from admin networks; no unexplained accounts or SSH changes.

GREYNOISE · GT13 · CHECK POINT SMS · CVE-2026-16232

Firewall managers raided, with AI suspected at the controls

GreyNoise watched an unknown actor run more than 100 tasks across Check Point management servers, copying the keys that make a firewall trustworthy.

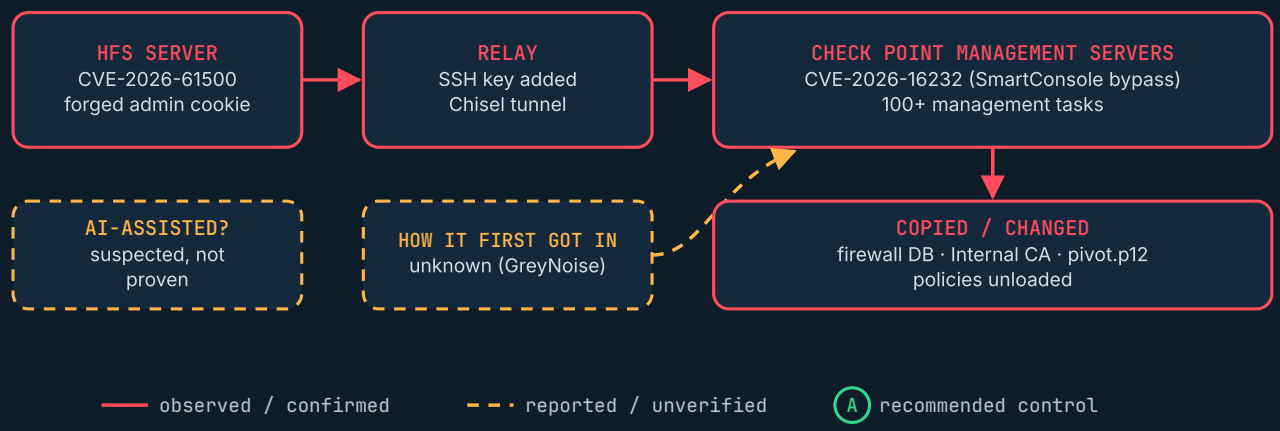


Figure 2 · GT13's path as GreyNoise reconstructed it. The first route to the Check Point servers is unknown; AI use is GreyNoise's suspicion [2]. MAG212 CYBER diagram.

WHAT HAPPENED

In a 23 November post, GreyNoise described an actor it calls GT13, with no known group, motive or country. Between 2 October and 2 November it reached at least 22 organisations in 17 countries, in finance, energy, government, transport, mining, engineering and manufacturing, and used 24 Check Point Security Management Servers. [2]

Using a script for CVE-2026-16232, a SmartConsole authentication bypass patched in July 2026, it ran tasks that copied firewall databases and the Internal CA, minted a certificate called pivot.p12 and unloaded security policies. GreyNoise could not tell how GT13 first reached the Check Point servers, and expects the intrusion is ongoing. [2][3]

THE AI QUESTION

GreyNoise "suspects" agentic tooling, citing automated checks, odd timeline gaps and output written in IP order. It presents this as evidence, not proof. [2]

CHECK YOUR MANAGEMENT SERVERS

- Confirm the CVE-2026-16232 fix is installed.
- Review management task history for exports of the firewall database or Internal CA.
- Look for unknown certificates (pivot.p12) and policy unloads.
- Check `/etc/ld.so.preload` for `/usr/lib/.libproc.so`.
- Audit `/root/.ssh/authorized_keys`.

INDICATORS (GREYNOISE)

- Domain `newpayapp.com` and subdomains.
- User-agent containing `research`.
- 99 IPs, mostly ExpressVPN (AS206092); full list in [2].

IF YOU FIND SIGNS

Treat credentials and Internal CA material as exposed: rotate, reissue certificates, and report to your national CERT. We found no Check Point statement as of this morning.

DRUPAL CORE · SA-CORE-2026-017 · CVE-2026-132165

Drupal's own installer is being used to take over sites

A "highly critical" flaw lets attackers reinstall a Drupal site under certain conditions. Exploitation began the day after the fix; CISA wants it closed by Friday.

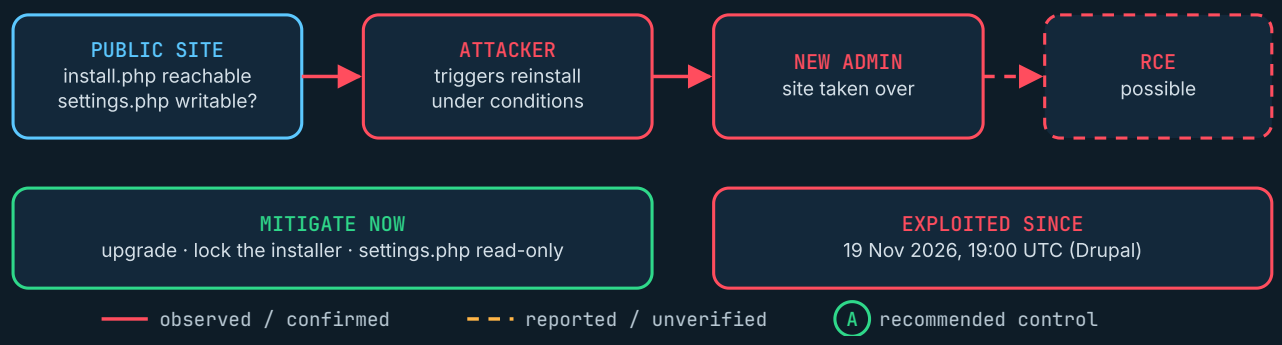


Figure 3 · How the reinstall attack works, per Drupal's advisory [4]. RCE is listed as possible, so it is dashed. MAG212 CYBER diagram.

WHAT HAPPENED

On 18 November Drupal's security team published SA-CORE-2026-017 (risk 20/25, "highly critical"). Under specific conditions, `install.php` can be used to try to reinstall Drupal, leading to site takeover or remote code execution. The team says it received a report of exploitation on live sites from 19 November, 19:00 UTC. CISA added it to KEV on 24 November, due 27 November. [4][5]

Drupal credits Anthropic's OSS Scanner with discovering the flaw. [4]

WHO IS AFFECTED

- Drupal 10 before 10.6.22.
- Drupal 11.0.0 up to 11.3.22, and 11.4.0 up to 11.4.13.
- End-of-life versions (11.2.x and below, 10.5.x and below, 8, 9) get no fix: upgrade.

FIX

BRANCH	UPDATE TO
11.4.x	11.4.13
11.3.x	11.3.22
10.6.x	10.6.22

IF YOU CAN'T UPGRADE TODAY

- Follow Drupal's guide to securing the installer.
- Make `settings.php` unwritable by the web server (covers some, not all, paths).
- Drupal Steward sites are protected against known vectors, but should still upgrade.

Linux · shell (site root) | web user | READ-ONLY | NOT TESTED BY MAG212

check one site

```
drush status --field=drupal-version
ls -l web/sites/default/settings.php
```

Shows the core version and whether settings.php is writable. Paths vary by install. Not tested by MAG212.

CHECK POINT RESEARCH · VOLANT MANTICORE · KUBOSHELL

Volant Manticore hides its commands in IPFS files

A new Iran-linked group poses as job seekers and seminar hosts, then steers its malware through a public file-pinning service.

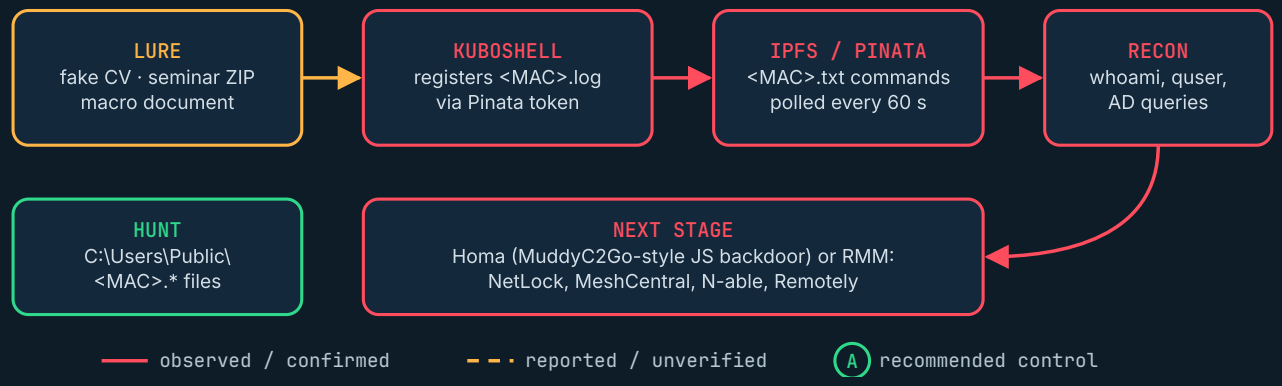


Figure 4 · Volant Manticore's chain as Check Point Research describes it [6]. MAG212 CYBER diagram.

WHO AND WHO IS TARGETED

Check Point Research (24 November) assesses with high confidence that Volant Manticore is an Iran-nexus group, and with medium confidence that it is historically linked to Iran's intelligence ministry and made up of former MuddyWater operators. It has targeted telecoms, airlines and critical infrastructure in Cyprus since September 2025, and shifted to Saudi healthcare in September 2026. [6][7]

HOW KUBOSHELL WORKS

KuboShell is a 64-bit Windows backdoor. It names each victim by its network adapter's MAC address, uploads a `.log` file through a hard-coded Pinata token, and every 60 seconds looks for a `.txt` command file, which it runs in hidden PowerShell. Operators used it for reconnaissance before deploying Homa or remote-management tools. [6]

SAMPLE INDICATORS

TYPE	VALUE (DEFANGED)
Domain	cnpcyprus[.]net
Domain	aegeneair[.]com
Domain	webmail-eac[.]com
IP	185.205.187[.]109
IP	185.253.118[.]221
SHA-256	684f748d…09ec9b250 (CV lure)

Selection from Check Point Research [6]; full tables in the report.

DEFEND

- Alert on Pinata and IPFS gateway traffic from hosts that never use them.
- Hunt for MAC-named files in the Windows Public user folder.
- Allow only approved RMM tools.
- Block macros; filter Catbox and Dropbox links in mail.

MAG212 suggestions from the report's findings.

Governments and services: what is confirmed, what is not

Four incidents from the last 48 hours. Each is labelled by how well it is sourced.

EU · OFFICIAL

European Commission: EU Academy users' data taken

The Commission said on 23 November that its investigation into an attack detected on 22 October found a data breach. Names and email addresses of EU Academy users, people outside the Commission, were exposed. Access is suspended and the EDPS was told. Scale is still under investigation; the Commission says the attack involved AI, and makes no attribution. [8][10]

EU · REPORTED · ANONYMOUS SOURCES

Euronews: China-backed group suspected

Citing two unnamed sources, Euronews reports the Commission internally suspects a China-backed group and that the breach is not fully contained. The Commission has not confirmed this. [9]

US · ONE ANONYMOUS SOURCE

An unclassified CIA system breached, AP source says

AP reported on 24 November, citing one person not authorised to speak, that an unclassified system handling open-source intelligence was breached, with no classified data involved and the issue resolved. No official CIA, ODNI or FBI statement. [11]

US · STATE · OFFICIAL

myColorado: data on nearly 150,000 people likely stolen

Colorado found the breach on 18 November and shut the digital ID app; it was still offline on 24 November. The state has not said what data or whether ransomware was involved. Residents were told to carry physical ID. [12]

UPDATE · OT

Peninsula Energy's 25 November update says the incident at its Lance uranium project in Wyoming is confined to plant and wellfield operating and control systems; operations are suspended. No attacker or ransomware has been named. [13]

WHAT TO DO WITH THIS

- EU Academy users: expect phishing that uses your name and the Commission's branding.
- Colorado residents: watch for messages about your digital ID; the state has not said what was taken.
- Everyone: an anonymous-source story is a reason to watch, not to act. Wait for scope before changing plans.

Patch board: five KEV deadlines this week

CISA added three flaws on 24 November, all due Friday 27 November, the day after Thanksgiving. Plan the work before the holiday.

CISA KEV: OPEN DEADLINES

CVE	PRODUCT	ADDED	DUE
CVE-2026-133968	MONAI Label	23 Nov	26 NOV
CVE-2026-134624	N-able Mail Assure	23 Nov	26 NOV
CVE-2026-132165	Drupal core	24 Nov	27 NOV
CVE-2026-132224	Optimizely Web Exp.	24 Nov	27 NOV
CVE-2026-131914	Idunno.AntiCsrf	24 Nov	27 NOV
CVE-2026-115731	Puppet Enterprise	17 Nov	1 Dec
CVE-2026-40217	BerriAI LiteLLM	18 Nov	2 Dec

KEV v2026.11.24 (1,795 entries), checked 06:53 PT 25 Nov; nothing added on 25 Nov at that time [5].

OPTIMIZELY: MOSTLY ON THE VENDOR

Attackers abused Optimizely's sign-up flow on 16 November to inject JavaScript into some customers' projects. The fix is server-side; Optimizely says it contacted affected customers. Check your account notices and review project code changes. [18]

IDUNNO.ANTICSRF: NO PATCH EXISTS

An abandoned ASP.NET module with an exploited deserialization flaw (CVSS 9.3). Find it in web.config files and remove it. [19]

STILL WAITING

ITEM	STATUS ON 25 NOV	ACTION
Tomcat CVE-2026-133325	11.0.30 NOT RELEASED	TLS 1.2 for cluster
PAN-OS CVE-2026-123633	HOTFIX STATUS UNCLEAR	disable HTTP/2
RHEL Ghostscript CVE-2026-125396	NO ERRATA LISTED	restrict uploads; watch
MONAI Label CVE-2026-133968	0.8.6 ON PYPI	upgrade by 26 Nov

Sources [20–23]. Vendor pages checked on 25 Nov.

Briefs

Shorter items and updates to stories we have covered this week.

SUPPLY CHAIN

Fake job tests hide malware in 13 NuGet packages

Socket found 13 malicious NuGet packages used in fake .NET “home assessment” projects; building the project runs the malware. One, WinUI.Button 1.0.0, was still listed when Socket published. No attribution. Never build a recruiter's project on a work machine. [16]

AI AGENTS

An AI coding agent found a decoy key in under 6 minutes

The Register reports that security firm Jesta caught an operator pointing the open-source OpenCode agent at a financial firm on 16 November. The agent followed a link found only in decoy documentation, tried planted keys, and was contained; nothing was stolen. [17]

AI SAFETY

Anthropic opens Enterprise Frontier Safeguards beta

Anthropic launched a public beta of cross-request misuse monitoring for zero-data-retention customers. Flags arrive as “Safety Cases” in the customer's own storage, which can feed a SIEM; Anthropic says it keeps no data and no humans review it. [15]

IDENTITY

Okta ties a vishing crew to a new leak site

Okta links the vishing cluster O-UNC-053 to the INCEPTION leak site and says it may be a ShinyHunters rebrand; INCEPTION denies it. The crew's “legal department” calls are this week's awareness lesson (p. 12). [14]

UPDATE · MSP

N-able: root cause still due

N-able says attackers reached one hosted server behind Mail Assure and SpamExperts, with no evidence customer data was taken. A root-cause report is promised within two weeks of 22 November. The related CVE-2026-134624 is due on KEV tomorrow. [24][5]

UPDATE · CLOUD

Azure APIM and GL.iNet: no new primary details

No Microsoft advisory, CVE or new NSM update for the Azure API Management secrets theft, and no CVEs yet for GL.iNet's GoodCloud flaws. Our 24 November playbooks still apply.

Your work list before the holiday

Ordered by urgency. Two KEV deadlines fall on 26 and 27 November, around Thanksgiving.

WHEN	TEAM	ACTION	SEE
TODAY	Virtualisation	Restrict vCenter and ESX management to admin networks; plan the VMSA-2026-0011 upgrade	p.04
TODAY	Web	Upgrade Drupal or lock the installer; check for reinstall activity since 19 Nov	p.06
TODAY	Network security	Confirm CVE-2026-16232 fix on Check Point managers; review task history	p.05
BY 26 NOV	Research / MSP	MONAI Label 0.8.6; confirm N-able guidance followed	p.09
BY 27 NOV	Web / dev	Remove Idunno.AntiCsrf; check Optimizely notices	p.09
THIS WEEK	SOC	Hunt for Pinata/IPFS traffic and MAC-named files in the Public folder	p.07
THIS WEEK	Identity	Move admins and help desk to passkeys; warn staff about “legal” calls	p.12
THIS WEEK	Dev	Block building untrusted job-test projects on work machines	p.10

ONE-PAGE HUNT SHEET

vCenter	new SSO users, roles, SSH enabled on hosts, unexpected snapshots or exports
Check Point	pivot.p12 · policy unloads · /usr/lib/.libproc.so in ld.so.preload · newpayapp.com
Drupal	unexpected install.php requests · new admin accounts · changed settings.php
Volant	Pinata / IPFS gateway traffic · MAC-named files in Public · new NetLock or MeshCentral
Vishing	new legal- lookalike domains · MFA pushes after phone calls

BEFORE YOU CLOSE A TICKET

- vCenter and ESX builds match VMSA-2026-0011.
- Drupal reports 10.6.22, 11.3.22 or 11.4.13.
- Check Point managers show the July fix; CA rotated if touched.
- pip show monailabel reports 0.8.6.
- Idunno.AntiCsrf gone from every web.config.

COMMAND SAFETY

Every command in this issue is read-only. They are generic checks built from vendor or researcher guidance. None was run by MAG212 for this issue; try them on one system first.

The “legal department” is calling

A five-minute lesson for every employee, with notes for administrators and business leaders.



Figure 5 · The O-UNC-053 vishing playbook as Okta and Unit 42 describe it, via The Hacker News [14]. MAG212 CYBER diagram.

WHAT IS HAPPENING

Callers claiming to be from your company's legal department or help desk steer staff to a lookalike sign-in page, often on a domain like legal-yourcompany.com registered the day before. The page passes your real login through, and the caller asks you to read out a code or approve a prompt. Unit 42 counts more than 70 such domains since October. [14]

FOR EVERY EMPLOYEE

- No one from legal, IT or security needs your one-time code. Ever.
- Don't approve a sign-in prompt you didn't start.
- Hang up and call back on a number from the intranet or directory.
- Report the call, even if you did nothing wrong.

FOR ADMINISTRATORS

- Move privileged and help-desk accounts to passkeys first; Okta says the kit can't bypass passkeys or FastPass [14].
- Watch for newly registered domains containing your brand plus “legal”.
- Alert on MFA approvals that follow a burst of denied prompts.

FOR BUSINESS LEADERS

- Fund phishing-resistant MFA for the people attackers call first.
- Make “call back on a known number” a rule, not a suggestion.
- Thank people who report; never punish them.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Who in our company would get this call first?
2. Could a caller reset an account by phone today?
3. How fast would we spot a lookalike domain with our name in it?

Sources

[1] Broadcom · 24 Nov 2026 · VMSA-2026-0011: VMware ESX, vCenter, Workstation, Fusion, Tools and Avi updates

[2] GreyNoise (Steve Miller) · 23 Nov 2026 · 99 IPs but a C2 ain't one: GT13 Check Point Security Management Server intrusion campaign

[3] SecurityWeek · 24 Nov 2026 · Check Point Security Management servers hacked in AI-assisted campaign

[4] Drupal Security Team · 18 Nov 2026, updated 21 Nov · SA-CORE-2026-017: Drupal core, highly critical, remote code execution

[5] CISA · checked 25 Nov 2026, 06:53 PT · Known Exploited Vulnerabilities catalog (JSON v2026.11.24)

[6] Check Point Research · 24 Nov 2026 · Volant Manticore: flying under the radar

[7] The Hacker News · 24 Nov 2026 · Iran-aligned Volant Manticore uses IPFS-based KuboShell backdoor

[8] European Commission · 23 Nov 2026 · Midday briefing video (spokesperson Thomas Regnier)

[9] Euronews · 23 Nov 2026 · China-backed hackers suspected behind ongoing EU Commission cyberattack

[10] SecurityWeek · 24 Nov 2026 · European Commission uncovers data breach in cyberattack investigation

[11] SecurityWeek (AP) · 24 Nov 2026 · An unclassified CIA system was breached in a cyberattack, AP source says

[12] The Record · 24 Nov 2026 · myColorado app down after data breach

[13] SecurityWeek · 24 Nov 2026, updated 25 Nov · Peninsula Energy halts trading after cyber incident hits US uranium mine

[14] The Hacker News · 24 Nov 2026 · Okta links ShinyHunters-associated vishing cluster to INCEPTION leak site

[15] Anthropic · 23 Nov 2026 · Zero data retention with Enterprise Frontier Safeguards

[16] Socket · 23 Nov 2026 · Malicious NuGet packages in fake job assessments

[17] The Register · 24 Nov 2026 · An AI coding agent found a financial firm's access key in under 6 minutes

[18] Optimizely · Nov 2026 · Status incident (CVE-2026-132224)

[19] Mandiant · 18 Nov 2026 · MNDT-2026-0048: Idunno.AntiCsrf (CVE-2026-131914)

[20] Apache Tomcat · checked 25 Nov 2026 · Fixed in Apache Tomcat 11.x (CVE-2026-133325)

[21] Palo Alto Networks · checked 25 Nov 2026 · CVE-2026-123633: PAN-OS impact of nginx HTTP/2 vulnerabilities

[22] Red Hat · checked 25 Nov 2026 · CVE-2026-125396 (Ghostscript)

[23] PyPI · 22 Nov 2026 · monailabel release history (0.8.6)

[24] The Hacker News · Nov 2026 · N-able confirms hackers accessed cloud server

HOW WE VERIFIED THIS ISSUE

- Read directly: Broadcom VMSA-2026-0011, GreyNoise's GT13 post, Drupal SA-CORE-2026-017, Check Point Research's Volant Manticore report and the CISA KEV JSON.
- The European Commission statement comes from its 23 November briefing video and press coverage; no written release was found. Euronews' attribution claim and AP's CIA report rest on anonymous sources and are labelled so.
- Okta and Unit 42 details come via The Hacker News; we found no Check Point statement on GT13 as of this morning. PAN-OS hotfix and RHEL Ghostscript status could not be confirmed.
- No command in this issue was executed by MAG212.

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