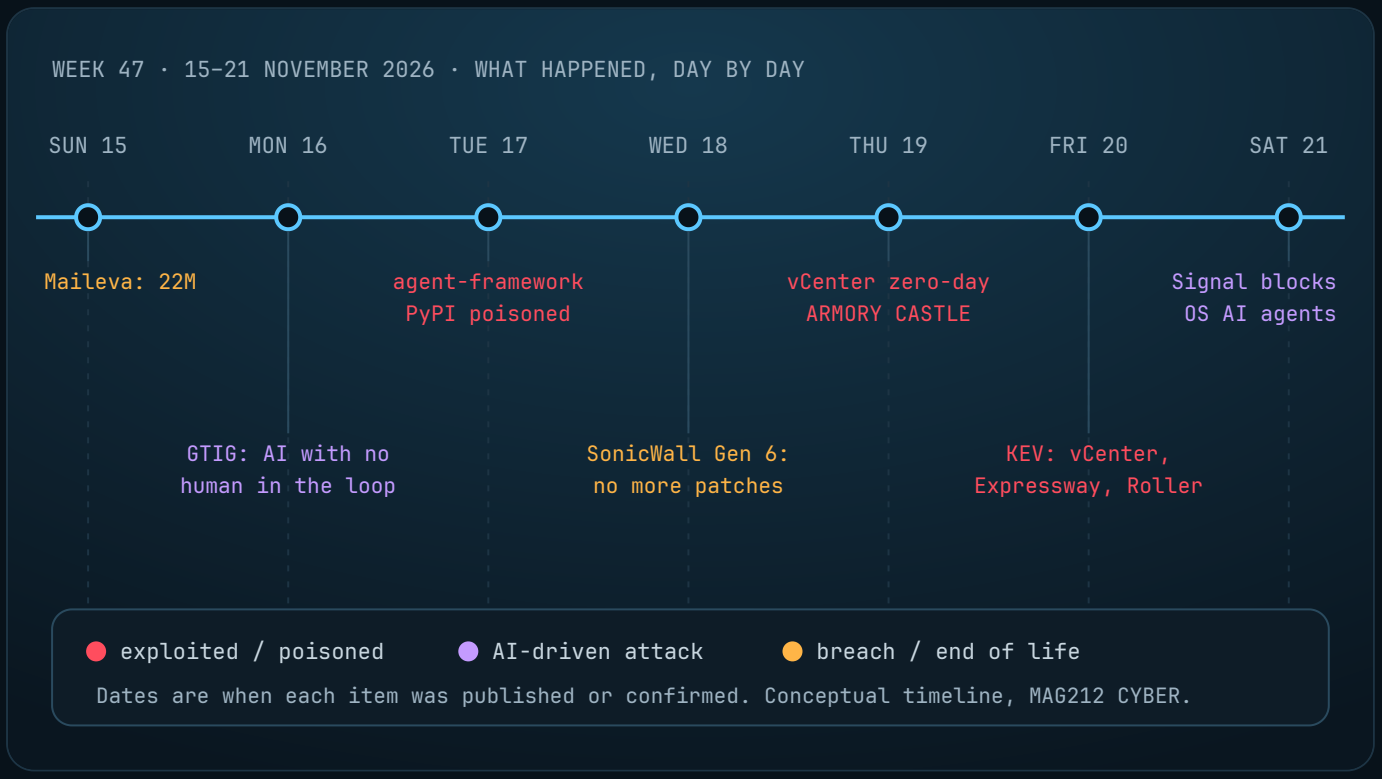
MAG212 CYBER

WEEKLY

Saturday, 21 November 2026

WEEK OF 15–21 NOV · CUTOFF 7:00 AM PT



THE WEEK IN CYBER · 15–21 NOVEMBER

Machine speed

Google and Amazon documented AI agents finding and exploiting bugs with no human steering each step. A Chinese espionage group owned vCenter with a zero-day. And most of the week's big breaches came in through a supplier. Here is what changed, what is confirmed, and what to fix first.

04 KEV board: vCenter, Expressway, Roller due 23 Nov

05 vCenter zero-day: ARMORY CASTLE's chain

09 AI agents that hack without a human

11 The supplier was the way in

12 Breach ledger: confirmed vs claimed

14 OT week: fridges, brakes, PLCs

9
flaws added to CISA KEV, 17–20 Nov

23 NOV
federal deadline: vCenter, Expressway

11 MIN
Cairn agents: API map to file write

1.6M+
people in SBC's largest category

What mattered this week

Developments published or confirmed 15–21 November 2026; earlier items are dated as such.

Infrastructure under fire

Broadcom fixed a vCenter authentication bypass that Google says ARMORY CASTLE exploited since September. On 20 Nov CISA put it, Cisco Expressway and Apache Roller on KEV with a 23 Nov deadline. [5][1]

AI agents went operational

GTIG saw attackers automate discovery and exploitation "without a human in the loop for the first time". Amazon says Chinese-nexus Cairn agents found a MONAI Label zero-day on their own. [20][18]

Breaches through suppliers

Uber, Cursor and Notion via Fireworks AI; JPMorgan, Visa and Mastercard via unnamed vendors; Infoblox via a migration vendor; 40+ Irish credit unions via Wellington IT. [33][36][35][38]

End of life and end of patience

SonicWall will not patch Gen 6 at any severity. Project Zero will publish bug details 90 days after reporting, fixed or not. [57][26]

THE THREE PRIORITY ACTIONS

1. **Meet the 23 Nov KEV deadline: vCenter, Expressway, Roller, SAP.**
   vCenter to 8.0 U3m / 9.0.2.0200 / 9.1.1.0200; Expressway to X15.5.20; Roller to 6.1.6+. Hunt before you patch: patching does not remove an intruder. [1][4][9]
2. **Put AI gateways and agent servers under production controls.**
   Authentication on, no public exposure, spend alerts, rotate provider keys. MONAI Label has no fixed release: block untrusted access now. [21][19]
3. **Inventory supplier keys and tokens, and retire the ones nobody owns.**
   Barracuda's breach started with an AI-vendor key it never retired; agent-framework stole CI and cloud tokens. [23][29]

STATUS AT A GLANCE

ISSUE	STATUS	ACT BY
vCenter CVE-2026-123890	EXPLOITED · ZERO-DAY	23 Nov (KEV)
Cisco Expressway CVE-2026-76466	EXPLOITED (F6) · KEV	23 Nov (KEV)
MONAI Label (GHSA, no CVE yet)	EXPLOITED · NO FIXED RELEASE	isolate now
SonicWall Gen 6	NO MORE PATCHES	plan replacement

CONTENTS

03 The week, day by day
04 KEV board
05 vCenter zero-day
06 vCenter: patch, hunt, evict
07 Cisco Expressway
08 Server bugs scorecard
09 AI agents that hack
10 Defending against AI agents
11 The supplier was the way in
12 Breach ledger
13 Incidents and outages
14 OT and ICS
15 Patch roundup
16 Nation-states, arrests, policy
17 Defender's Action Desk
18 Awareness lesson
19 Sources

Seven days in twelve lines

Each line is dated by when the item was published or confirmed, not when the attack happened. Several incidents began weeks earlier.

SUN 15	●	Maileva (La Poste) confirms 22M mail recipients' names and addresses taken in September. [40]
MON 16	●	GTIG AI Threat Tracker: exploit_agent diffs patches and exploits them automatically; MIDNIGHT NEPTUNE backdoors Claude Code settings. [20]
MON 16	●	Uber files: 149,346 people affected via Fireworks AI. Coles, Ipsos and Infoblox disclose incidents. [33]
MON 16	●	BIS interim final rule on remote access to advanced chips. Alleged INC/Lynx affiliate in US court after extradition. [70]
TUE 17	●	Two poisoned agent-framework releases on PyPI for about an hour. OPTIMJACK code served to 178+ sites until patched. [29]
TUE 17	●	CISA adds Puppet CVE-2026-115731 to KEV. Java4Shell disclosed. Equinor reports an ongoing attack. [1]
WED 18	●	SonicWall ends all Gen 6 patching. SBC Medical files 8-K. N-able confirms a Mail Assure server breach. Ruby fixes Ruby2Shell. [57]
WED 18	●	KEV adds Apache Axis, REDCap, Synology DSM (due 21 Nov) and LiteLLM (due 2 Dec). [1]
THU 19	●	Broadcom fixes vCenter CVE-2026-123890; GTIG ties zero-day use to ARMORY CASTLE. F6 reports Expressway breaches. Commission confirms an “AI generated” campaign. [5]
FRI 20	●	KEV adds vCenter, Expressway, Roller and SAP NetWeaver, due 23 Nov. Equinor says its attack has been stopped. TfL Oyster breach: ~265,000 people. [1]
FRI 20	●	Amazon: Chinese-nexus Cairn agents found and exploited a MONAI Label zero-day after an operator set only the goal. [18]
SAT 21	●	GnuPG fixes a critical GPGME double free. Signal blocks screenshots by default to stop OS AI agents reading chats. [62]

BEFORE THE WEEK, STILL LANDING

- FBI FLASH on the ARTEX AI framework (13 Nov): some intrusions went from targeting to privileged access in under three hours. [22]
- Amazon on ARTEX agents stealing AI provider keys (13 Nov); Barracuda's 44-hour, ARTEX-linked cloud intrusion (11 Nov). [21][23]
- Project Zero's “Full 90” policy (13 Nov): details published 90 days after report, fixed or not. [26]

CATALOG 2026.11.20 | 9 ADDITIONS 17–20 NOV | BOD 26-04

NOT IN KEV: nginx2root, Java4Shell, Drupal

What CISA says is being exploited

The KEV catalog lists vulnerabilities with evidence of exploitation. US federal agencies must fix them by the due date; everyone else should treat the list as a floor, not a ceiling.

ADDED	DUE	CVE	PRODUCT	WHAT IS KNOWN
20 Nov	23 Nov	CVE-2026-123890	VMware vCenter	Zero-day since Sept; ARMORY CASTLE (GTIG)
20 Nov	23 Nov	CVE-2026-76466	Cisco Expressway	1 org, 4 devices (F6); Cisco advisory still v1.0
20 Nov	23 Nov	CVE-2026-129448	Apache Roller	Apache: “being actively exploited”; no actor
20 Nov	23 Nov	CVE-2025-42884	SAP NetWeaver EP	Nov 2025 JNDI bug, CVSS 6.5; no public details
18 Nov	21 Nov	CVE-2026-90436	Apache Axis 1.x	Used against Confluence DC; Axis 1 is EOL
18 Nov	21 Nov	CVE-2026-90817	REDCap	Used to drop XMRig miners
18 Nov	21 Nov	CVE-2024-10441	Synology DSM	Used for C3RB3R ransomware on NAS
18 Nov	2 Dec	CVE-2026-40217	LiteLLM	LLMjacking: Virtual Key to admin
17 Nov	1 Dec	CVE-2026-115731	Puppet Enterprise	Report deserialization RCE; one public user report

Table 1 · CISA KEV additions 17–20 November, from the official catalog data (GitHub mirror, version 2026.11.20) [1] and The Hacker News [2, 3]. cisa.gov itself was unreachable from our tools.

WHAT CHANGED

- Every new entry now cites CISA's BOD 26-04 and “Forensics Triage Requirements”. Internet-facing items exploited in the wild got three-day deadlines. [1]
- KEV now corroborates GTIG on vCenter and F6 on Expressway, closing the gap our 20 Nov daily flagged. [1] [2]
- SAP's CVE-2025-42884 is a year old. The Hacker News found no public report of how it is being exploited. [2]

DUE NEXT WEEK (ADDED EARLIER)

ADDED	DUE	CVE	PRODUCT
10 Nov	24 Nov	CVE-2026-124194	Microsoft Outlook (Patch Tuesday zero-day)
10 Nov	24 Nov	CVE-2026-125350	Google Chrome

HOW TO USE THIS BOARD

1. Search your asset inventory for each product, including appliances and lab or DR copies.
2. Patch internet-facing and identity-adjacent systems first: vCenter, Expressway, Roller, SAP portals.
3. Where you cannot patch by the due date, remove exposure (firewall, disable the endpoint) and log the exception.
4. Hunt for compromise on every listed system that was exposed before you patched.
5. Re-check the catalog: CISA adds entries on weekdays.

FIXED 19 NOV · VMSA-2026-0009 | CVSS 9.8 | EXPLOITED AS ZERO-DAY (GTIG)

CISA KEV 20 NOV · DUE 23 NOV

vCenter zero-day: from directory port to domain secrets

KEY FACT **What happened.** On 19 November Broadcom fixed CVE-2026-123890, an authentication bypass in vCenter's VMware Directory Service reached over DCE/RPC on TCP 2012. An unauthenticated attacker becomes administrator@vsphere.local. Google's GTIG and Mandiant say the flaw was exploited as a zero-day from early September and attribute the activity to "the suspected PRC-nexus espionage actor ARMORY CASTLE (formerly tracked as UNC5221)". [4][5]

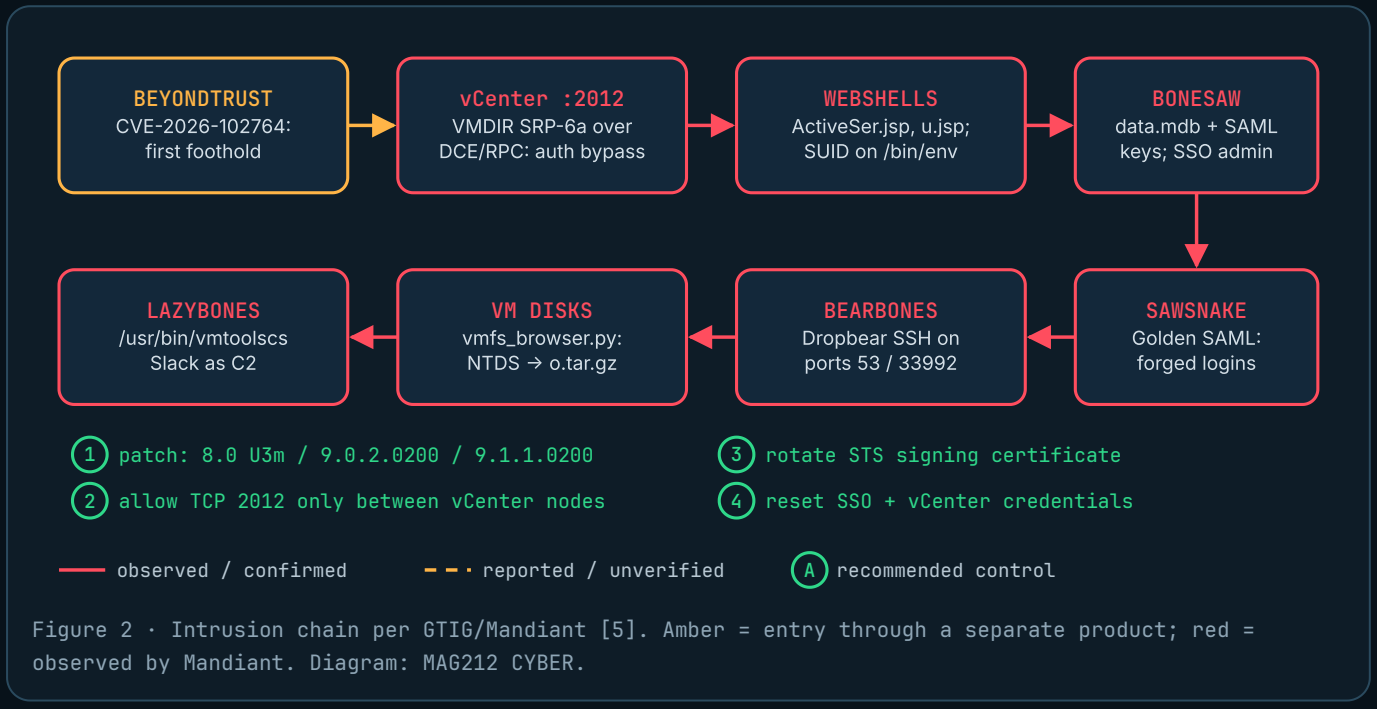


Figure 2 · Intrusion chain per GTIG/Mandiant [5]. Amber = entry through a separate product; red = observed by Mandiant. Diagram: MAG212 CYBER.

HOW THE ATTACK WORKS

The bug sits in the SRP-6a password exchange of the directory service. Once in as SSO administrator, the actor dropped JSP webshells, set SUID on `/bin/env`, and ran BONESAW to copy the directory database (`data.mdb`) and SAML signing keys and to create an SSO admin. SAWSNAKE then forged "Golden SAML" logins. [5]

To stay in, it added a rogue `sps-*@vsphere.local` account, toggled SSH through the appliance REST API, and installed two backdoors. It used `vmfs_browser.py` to read Windows domain controllers' disks directly and pull NTDS. [5]

WHAT IT TAKES

- Network reach to TCP 2012 on vCenter. In Mandiant's case the actor got that reach through a BeyondTrust flaw (CVE-2026-102764). [5]
- No credentials and no user action. Broadcom lists no workaround; the fix is not available as a Quick Patch. [4] [4]
- vCenter 7.0 has no public fixed build: Broadcom says to contact support. [4]

WHO AND WHY

GTIG calls the actor espionage-focused. Victim names and counts are not public; Mandiant CTO Charles Carmakal spoke of "multiple incidents". On 20 November CISA added the CVE to its Known Exploited Vulnerabilities catalog with a 23 November federal deadline. [5][1]

vCenter: patch, hunt, evict

VMSA-2026-0009 also fixes SDDC Manager (CVE-2026-123891/2/3) and VMware Tools (CVE-2026-123894).

PRODUCT	FIXED VERSION	NOTE
vCenter Server 9.1	9.1.1.0200	no workaround
vCenter Server 9.0	9.0.2.0200	no workaround
vCenter Server 8.0	8.0 U3m	not a Quick Patch
VMware Cloud Foundation 5.2	5.2.5	updates bundled vCenter
vCenter Server 7.0	none public	contact Broadcom support

Table 2 · From Broadcom's VMSA-2026-0009.1 [4] and Rapid7 [6]. Check the advisory for your exact build before you upgrade.

PowerCLI · vCenter admin · READ-ONLY · NOT TESTED BY MAG212

VERSION + ROGUE ACCOUNT

```
Connect-VIServer vcenter.example.com
$global:DefaultVIServer.Version
$global:DefaultVIServer.Build
Get-VIAccount |
  Where-Object { $_.Name -like 'sps-*' }
```

From Ostorlab's write-up, not a Broadcom procedure. Compare the build with the VMSA. Any `sps-*` account you did not create matches GTIG's rogue-account pattern. Not run by MAG212. [7][5]

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

HOST INDICATORS

```
ls -la /tmp/123 /tmp/sss /tmp/dbr \
  /usr/bin/vmtoolscs 2>/dev/null
ls -l /bin/env     # SUID 's' bit?
ss -ltnp | grep -E ':(53|33992) '
# from a user LAN host:
nc -vz vcenter.example.com 2012
```

MAG212 triage suggestion built from GTIG's file and port indicators and Ostorlab's reachability test. The last line should FAIL from ordinary networks. A hit means incident response, not cleanup. [5][7]

INDICATORS (GTIG)

FILES	ActiveSer.jsp · u.jsp · /tmp/123 · /tmp/sss · /tmp/dbr · /usr/bin/vmtoolscs · o.tar.gz
SSH	banner SSH-2.0-pulsesecure_23345 · ports 53, 33992
ACCOUNT	sps–<random>@vsphere.local
IPs	11 “suspected obfuscation network” IPs, e.g. 103.147.251[.]5, 103.190.38[.]3 — full list and YARA rules in [5]

No file hashes are public; GTIG keeps full IoCs in a registered collection. [5]

CONTAIN, FIX, VERIFY

1. Restrict TCP 443, 2012, 22 and 5480 to admin and peer networks (Mandiant vcsa-hardening-tool).
2. Patch every vCenter, including lab and DR instances.
3. If any indicator hits: rotate the STS signing certificate, reset SSO and vCenter credentials, and treat AD as exposed.
4. Verify: new build number; TCP 2012 unreachable from user networks.
5. Check BeyondTrust appliances for the entry bug.

EXPLOITED (F6) · CISA KEV 20 NOV | CVSS 9.8 · CWE-798 | PUBLIC POC SINCE 5 NOV | CISCO ADVISORY STILL v1.0

Cisco Expressway: a static password, four breached devices

KEY FACT **What happened.** Cisco fixed CVE-2026-76466 on 21 October: clustered Expressway-C and Expressway-E accept a hard-coded credential that gives an unauthenticated attacker root. On 19 November Russian security firm F6 reported that attackers used it against one Russian organisation and compromised four devices. On 20 November CISA added it to KEV (due 23 November), yet Cisco's advisory, checked 21 November, is still version 1.0 and still says PSIRT is not aware of malicious use. F6's own report did not load; details come from SecurityWeek and Ostorlab. [9][10][1]

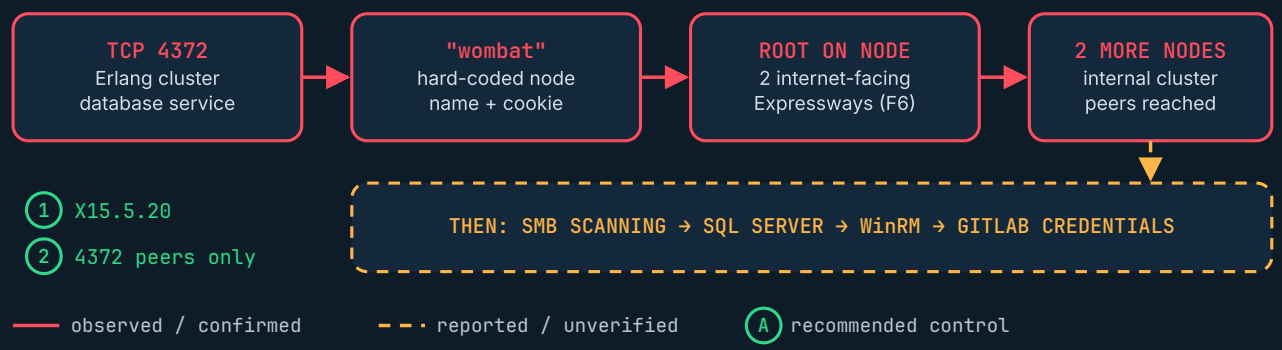


Figure 3 · Exploitation path. Red = reported by F6 [10]; amber dashed = post-compromise activity as reported. Mechanism per Ostorlab [11]. Diagram: MAG212 CYBER.

WHO IS AFFECTED

- Expressway-C and -E, virtual and appliance, **only when configured in a cluster**, on X15.5.3 and earlier or X14 and earlier. [9]
- Fixed in X15.5.20. X14 and earlier must migrate to a fixed release. Cisco lists no workaround. [9]
- Cisco blames persistent cookies and weak client-certificate checks when TLS Verify Mode is on for clustering. [9]

WHAT THE ATTACKERS DID

Per SecurityWeek's account of F6: entry through two internet-facing X15.5.3 devices, then two internal cluster nodes. Python tools whose code comments suggested an AI assistant scanned for SMB; the intruders then moved to SQL Server and WinRM and went after GitLab credentials. No attribution. [10]

INDICATORS (F6, SECOND-HAND)

IPs	66.179.31[.]32 · 18.130.47[.]116
LOG	wombat@127.0.0.1 in erlang.log
FILES	/mnt/harddisk/i<4 digits>[letter]/*.py

Expressway · root shell | root | READ-ONLY | NOT TESTED BY MAG212

HUNT

```
grep -R "wombat@127.0.0.1" \
  /var/log/ 2>/dev/null
find /mnt/harddisk -maxdepth 3 -type f \
  -name '*.py' 2>/dev/null \
  | grep -E '/i[0-9]{4}[A-Za-z]?/'
nc -vz expressway.example.com 4372
```

From Ostorlab, not Cisco: Cisco publishes no compromise checks. Any hit means incident response. The last line, run from a non-peer network, should fail. Not run by MAG212. [11]

WHY IT MATTERS

- A month passed between patch and reported attacks, and a public PoC appeared in between. [10] [11]
- Expressway sits at the edge for video and voice; a root shell there is a route inside. [10]

Exploited, attempted or just possible?

Seven server-side bugs made headlines this week. Only three have evidence of real exploitation. The difference decides what you patch tonight and what can wait for the next window.

BUG	STATUS ON 21 NOV	FIX	KEV
Apache Roller CVE-2026-129448 · 9.8	EXPLOITED (Apache)	6.1.6+; or disable XML-RPC	20 Nov
Puppet CVE-2026-115731 · 9.4	EXPLOITED (one public report)	PE 2026.0.1 / 2025.12.1 / 2023.8.13	17 Nov
SAP NetWeaver EP CVE-2025-42884 · 6.5	EXPLOITED (KEV; no details)	SAP Nov 2025 patch day	20 Nov
Java4Shell CVE-2026-114938 (OpenJDK)	ATTEMPTS ONLY	Oracle 8u513, 17.0.21.1, 21.0.13.1, 25.0.5.1	no
nginx2root CVE-2026-123007 · 9.2 (v4)	PUBLIC PoC, NO ATTACKS	OSS 1.30.7 / 1.31.9; Plus 37.0.8.1 / 37.3.0.1	no
F5 BIG-IP, six TMM flaws · 9.8	NOT EXPLOITED	Engineering hotfixes only	no
Drupal core CVE-2026-132165	PoC, NO ATTACKS	10.6.22, 11.3.22, 11.4.13	no

Table 3 · Status as of 21 November. Sources: KEV catalog [1], Apache via BleepingComputer [12], The Hacker News [13, 2, 16, 17], SecurityWeek [14, 15]. CVSS shown where a score is published; scorers differ.

APACHE ROLLER

Pre-auth deserialization through the XML-RPC endpoint in Roller 4.0.0–6.1.4. If you cannot upgrade, set `enabledForExtensions` to false and remove the `/roller-services/xmlrpc` mapping, then treat exposed servers as possibly compromised. [12]

PUPPET

Report deserialization RCE, fixed 3 November. The only public evidence is a user who traced an intrusion back to it after finding a misconfigured CA. Patch servers and check CA certificates you did not issue. [13]

JAVA4SHELL

Only on CPUs with AVX-512 VBMI. GreyNoise saw 150+ attack-shaped requests from 5 IPs and no successful intrusions; watchTowr calls the attempts “not particularly functional”. Cisco and Siemens products still await fixes; Siemens says take three Industrial Edge products offline. [14]

NGINX2ROOT

An HTTP/2 flow-control underflow in nginx 1.9.5–1.31.8. Censys reproduced it over cleartext HTTP/2 and counts about 9 million services on affected versions with HTTP/2 on. No in-the-wild use reported. Restart fully after patching; a reload keeps old workers. [15]

HOW TO READ “EXPLOITED”

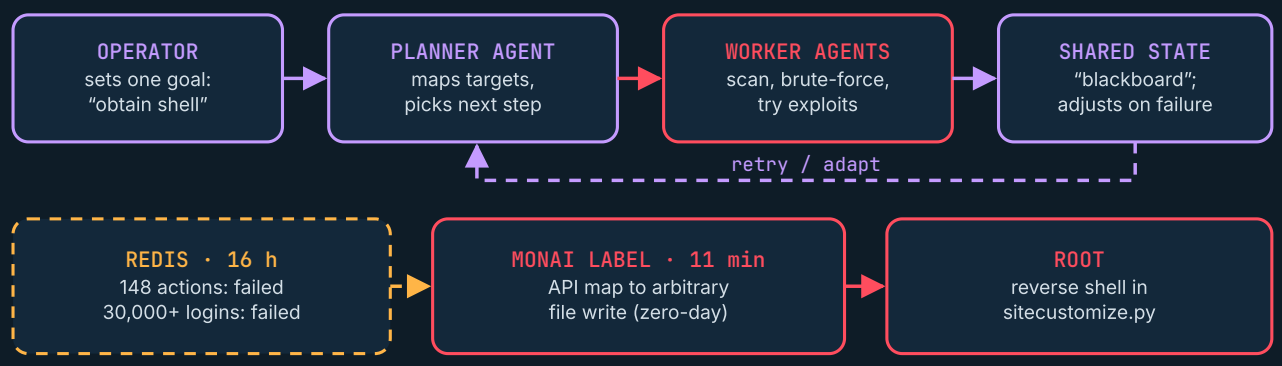
A public proof of concept means anyone can try. Attempts on sensors mean someone is trying. Exploited means a defender or vendor saw it work against a real system. Headlines blur the three; SecurityWeek's own page title called Java4Shell “exploited in the wild” while its text described attempts only.

AMAZON · 20 NOV | GTIG · 16 NOV | MONAI LABEL: NO FIXED RELEASE

ATTRIBUTION: MODERATE CONFIDENCE

AI agents that hack without a human at the keyboard

KEY FACT **What changed.** GTIG reported attackers using LLM frameworks "to fully automate vulnerability discovery and exploitation without a human in the loop for the first time." Four days later Amazon described Chinese-nexus actors (moderate confidence) whose Cairn agents found a zero-day on their own: a critical flaw in the MONAI Label medical-imaging server (advisory GHSA-qc22-rmgc-vg94; no CVE assigned yet). [20][18]



Cairn campaign as described by Amazon: 8–10 Sept 2026, East Asian university servers.
Solid red = observed exploitation · dashed amber = failed attempts · purple = agent roles

Figure 4 · Cairn agent workflow and timeline as reported by Amazon [18]. Diagram: MAG212 CYBER.

FOUR FRAMEWORKS, ONE PATTERN

- **exploit_agent** (GTIG): diffs popular web software before and after each patch, then writes and runs the exploit. No actor named; Russian-language comments. [20]
- **Cairn**: planner and worker agents sharing a "blackboard"; also seen in an intrusion against US aerospace. [20][18]
- **ARTEX**: FBI says some intrusions reached privileged access in under three hours; Amazon saw its agents stealing AI provider keys to pay for more attacks. [22][21]
- **LLMjacking**: LiteLLM CVE-2026-40217 turns a Virtual Key into admin; single-day fraudulent charges above $100,000. [20]

WHAT IS CONFIRMED, WHAT IS NOT

- Amazon: "high confidence" the MONAI bug was a zero-day; "moderate confidence" on the Chinese-nexus actor. Victims: university servers. [18]
- The European Commission says its attack was "an AI generated cyber campaign" using a public tool. That the tool was ARTEX is Politico's unconfirmed report. [24][25]
- Visibility came from attacker mistakes: an exposed exploit_agent server, an unauthenticated Cairn panel, ARTEX agents reporting to Amazon's decoys. GTIG: these frameworks "trade stealth for velocity." [20][21]

MONAI IPs `142[.]4.98.145 · 142[.]4.107.34 (8–10 Sept)`

11 min
Cairn: API map to file write on MONAI (Amazon)

< 3 h
some ARTEX intrusions: target to privileged access (FBI)

$100k+
single-day LLMjacking charges (GTIG)

11 / month
zero-days in 2026 vs 8 in 2025; 22 in August (GTIG)

Defending against AI agents, and your own

The attackers' advantage is speed, not new magic. The same unpatched services, exposed consoles and leaked keys are being found faster. Your own AI tooling is now part of the attack surface.

1 · AI GATEWAYS AND INFERENCE ENDPOINTS

- Amazon's ARTEX campaign hit LiteLLM, Dify, Langflow, RAGFlow, Open WebUI, Ollama and similar tools through default credentials, known CVEs and secrets left in client-side code. [21]
- Never expose them to the internet without authentication. Patch LiteLLM (CVE-2026-40217, KEV due 2 Dec).
- Set spend alerts on every model provider; rotate keys found in repos or front-end code.

2 · MONAI LABEL AND RESEARCH SERVERS

- No fixed PyPI release exists (latest 0.8.5); the fix is merged in source only. Authentication is off by default. [19]
- Block untrusted network access, enable authentication, run as non-root.
- Look for unexpected Python startup files such as sitecustomize.py and for unusual training jobs.

3 · CODING AGENTS IN YOUR REPOS

- GTIG: MIDNIGHT NEPTUNE (suspected North Korea) edited `.claude/settings.json` in victims' repos so that starting Claude Code downloaded the SOMBERMEME backdoor. [20]
- Review changes to agent configuration files like any CI change: code owners, required review, alerts.
- Audit GitHub tokens with assistant-like names; the actor named its tokens after Microsoft Copilot.

4 · AGENTS THAT BROWSE FOR YOU

- NebuSec showed one malicious webpage could take over Meta's Muse agent, read and alter its memory and, chained with a kernel bug, control its cloud VM. Lab test only; NebuSec says it is fixed. [27]
- Signal now blocks screenshots by default because OS-level AI agents “scan” the screen; it calls its remedy “incomplete”. [28]
- Give agents the least privilege and shortest-lived credentials you can.

THE PATCH WINDOW IS SHRINKING

Project Zero now publishes bug details 90 days after reporting, fixed or not, moving to 60 days in February 2027 and 30 in January 2028. Its reasoning: patch soak time “is no longer meaningful in a world where attackers can almost immediately determine bug details.” GTIG's exploit_agent does exactly that, diffing patches as they ship. Plan for days between fix and exploit on internet-facing systems, not weeks. [26][20]

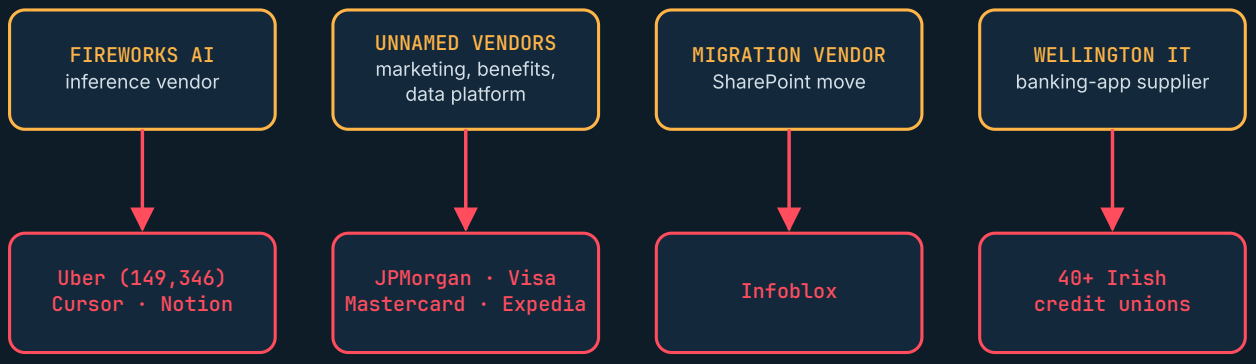
THREE QUESTIONS FOR YOUR TEAM

1. Which AI gateways, notebooks or model servers do we run, and are any reachable without authentication?
2. Who owns each AI provider key, where is it stored, and would we notice a $100,000 day?
3. Can a change to an agent's config file reach main without review?

MOST BIG BREACHES VIA SUPPLIERS | COUNTS: MOSTLY UNDISCLOSED | n0n CLAIMS UNVERIFIED

The supplier was the way in

KEY FACT **The pattern.** Most of the week's large incidents started at someone else's company. Victims rarely named the supplier, and almost every big number came from an extortion group, not a filing. [36][37]



Amber = the supplier that was breached or misused · red = the customer that disclosed. Counts as confirmed

Figure 5 · Supplier-to-customer paths disclosed this week [33, 36, 35, 38]. Diagram: MAG212 CYBER.

FIREWORKS AI → UBER, CURSOR, NOTION

Uber filed 149,346 people with the Texas attorney general, including driver's licence images, and named Fireworks as the provider. A Cursor key exposed through Fireworks was used against Cursor. [33][34]

n0n: JPMORGAN, VISA, MASTERCARD, EXPEDIA

All four blame unnamed third parties. Reuters found 16,000+ JPMorgan customer emails in the leak. Expedia's “nearly 1 billion records” is n0n's claim; its categories overlap and are not a count of people. Whether one vendor sits behind all four is not established. [36][37]

INFOBLOX AND WELLINGTON IT

Infoblox confirms access to company data through a vendor and says its products were not involved; stolen NIOS snapshots and staff data are reported, not confirmed. Wellington IT's breach in early October reached payee data in 40+ Irish credit unions' apps; they were told six weeks later. [35][38]

SOFTWARE SUPPLY CHAIN

Two agent-framework releases on PyPI (1.26.1, 1.26.2) stole cloud and CI tokens for about an hour on 17 Nov; Wiz counts three confirmed victims and Microsoft has given no root cause. OPTIMJACK pushed a wallet swapper, card skimmer and iPhone exploit loader through Optimizely to 178+ organisations. [29][31][32]

WHAT TO DO

- agent-framework: pin 1.26.0; do not uninstall with the infected interpreter (it re-runs the payload); rebuild, then revoke Entra sessions and review managed-identity and OIDC credentials. [30][29]
- Ask each critical supplier: what of ours do you hold, how would you tell us, how fast? Put the answers in the contract.
- Retire vendor keys when the project ends. Barracuda's breach began with one it never retired.

Confirmed versus claimed

The number in a headline is often the biggest one available, not the most accurate. This ledger separates what organisations or regulators confirmed from what attackers or reporters claimed.

ORGANISATION	CONFIRMED	CLAIMED / REPORTED	SOURCE
SBC Medical (Japan)	1,624,000 in largest category; categories overlap	“over 2 million” = categories added	[39]
Maileva / La Poste	22M mail recipients: names, postal addresses	Some payment reminders read	[40]
Transport for London	~265,000 Oyster photocard holders; no passwords or payments	—	[41]
Uber (via Fireworks)	149,346 people, incl. licence images	—	[33]
RIKEN Fugaku	4,222 + 375 users; SSH keys from users' PCs; offline since 14 Nov	—	[42]
Rakuten Securities	test environment accessed 11 Nov	up to 11.25M accounts' login IDs may be exposed	[43]
JPMorgan / Visa / Mastercard	marketing / email data at vendors; no counts	Reuters: 16,000+ JPMorgan emails	[36]
Expedia	intrusion via data-platform provider; no figures	n0n: “nearly 1 billion records”	[37]
Infoblox	company data via vendor; no counts	NIOS snapshots, staff SSNs (The Register)	[35]

Table 4 · Breaches disclosed or updated 15–21 November. Confirmed = stated by the victim, a filing or a regulator notice.

WHY THE NUMBERS DIFFER

- Category counts overlap: one patient can appear in reservations, inquiries and reviews.
- Records are not people: Expedia's claimed loyalty, account and profile tables describe the same customers.
- Dates differ: Maileva's breach happened in September; only the disclosure fell this week.

IF YOUR DATA WAS IN ONE OF THESE

- Change reused passwords and security answers (TfL exposed security questions and answers).
- Expect phishing that quotes the breach, your booking or your bank.
- Fugaku users: rotate SSH keys and access keys stored on the computers you used.

NOT THIS WEEK, DESPITE THE SEARCH RESULTS

Several breaches that search engines surface next to this week happened earlier: Maersk (11 Nov), Baker Tilly (11 Nov), Nitori (10 Nov), Iris Ohyama (8 Nov), Apify (9–12 Nov) and DreamHost (4 Nov). Two news URLs overstate counts tenfold: Nitori reported up to 37.62 million records and Iris Ohyama about 7.7 million people. Check the article text, not the link.

Disruptions and what we know about them

Six incidents that moved this week. Several are still under investigation; we report only what the organisations or named sources said.

European Commission

AI-ASSISTED

"An AI generated cyber campaign" using a public tool; detected 22 Oct, largely contained; several applications taken down, most restored. No attribution, no ransom. Politico's anonymous source names ARTEX and claims large data loss; the spokesperson says there is no evidence of a breach affecting staff "as a whole". [24][25]

Equinor (Norway)

STOPPED 20 NOV

An attack on some IT systems from 17 Nov; "has now been stopped" at 08:55 CET on 20 Nov. Production normal, no sign data was stolen; it "does not appear to be specifically targeting Equinor". [44]

N-able Mail Assure / SpamExperts

PORTAL DOWN

One hosted-cloud server accessed; management UI, APIs, quarantine and logging off in three regions while mail still flows. No evidence of customer data access. [45]

West Virginia Legislature

ONGOING 20 NOV

Website down and some IT systems disabled from 19 Nov; limited to the Legislature's own systems. No claim, and no answer on ransomware. [49]

Nvidia

CLAIM ONLY

The Gentlemen ransomware group lists Nvidia with a 28 Nov countdown and no proof. Nvidia: an incident "may have affected a third-party partner"; no sign its systems were hit. [46]

NSA network outage

NOT A CYBERATTACK

NSANet degraded on 17 Nov; officials blame maintenance. The National Cyber Director, Sean Cairncross, is out after a string of outages; officials see no coordinated attack. [51]

ALSO UNDER INVESTIGATION

- Coles (Australia) and Ipsos (France) disclosed incidents on 16 Nov; neither has found evidence of customer data loss or updated since. [48][47]
- Fugaku remains offline after malware was planted and user SSH keys were taken; no restoration date. [42]

LESSON

Several organisations disclosed within a day or two and updated as facts changed. That is good practice, and it is also why first reports so often change: plan your own incident communications around regular, dated updates.

CISA ICS: 17 + 19 NOV BATCHES | SEVERAL WILL NEVER BE FIXED

SECONDARY SOURCES (cisa.gov unreachable)

Fridges, brakes and PLCs: the unpatchable week

Industrial and building equipment stays in service for decades. This week's advisories show the result: serious flaws in products whose vendors have stopped fixing them.

PRODUCT	ISSUE	FIX STATUS	EXPLOITATION
Danfoss AK-SM 800A (supermarket refrigeration)	6 pre-login RCE flaws (Midnight Blue); details withheld	no patch mentioned	not reported
Copeland XWEB EVO	14 flaws incl. unauth command injection (CVE-2026-124010, 9.8)	5.6.2 / 5.7.0; credential flaws in final 5.8.8 never fixed	probing seen; no compromise confirmed
Elecbrakes EB2 / VM1 / ELBC2000 trailer brakes	Bluetooth control of brakes (CVSS 9.6 v3.1)	EB2 3.0.4.4.3; VM1 1.3.4.2.1; ELBC2000 EOL, no fix	not reported
OpenPLC Runtime ≤ 4.2.4	race condition creates admin accounts without login	no fix identified	not reported
libumqtt ≤ 1.1.1	integer underflow: DoS, memory corruption	unclear	not reported
Siemens (about nine advisories, 17 Nov)	SIMATIC, WinCC, RUGGEDCOM APE1808, ROS#, Femap	see each advisory	not reported
GeoVision GV-VMS camera software	abused to plant XMRig at ~13 organisations (Huntress)	no CVE, no patch	confirmed miner campaign

Table 5 · OT/ICS issues disclosed or active 12–21 November. Sources: The Hacker News [53], SecurityWeek [52], TheHackerWire [54], Security Boulevard [55], Huntress [56]. CISA advisory pages could not be read directly.

WHY REFRIGERATION MATTERS

Attacks on supermarket refrigeration hit about 700 French stores in October and more than 100 stores across Europe in early November; nobody has claimed them and the entry method is unexplained. This week brought no new wave, but it did bring flaws in two of the controller families used in stores. Copeland's controllers were probed within hours of disclosure. [52]

WHAT TO DO

1. Take controllers and PLC web interfaces off the internet; reach them only through a VPN or jump host.
2. Inventory end-of-life devices (ELBC2000, XWEB EVO on 5.8.8) and plan replacement.
3. Change default and shared passwords; Copeland's hard-coded admin password cannot be changed, so isolate.
4. For GeoVision servers, look for update.exe or ApplyUpdate.exe launched from the GeoVision service.

Everything else you should schedule

Important fixes with no confirmed exploitation, plus one product line that will get no fixes at all.

PRODUCT	WHAT	FIXED IN	EXPLOITED?
SonicWall Gen 6 / 6.5	No patches at any severity from 18 Nov	replace (Gen 8)	policy change
N-able N-central	17 CVEs; agents and probes must also upgrade	2026.4 HF3	not for these 17
Splunk Enterprise	unauth cluster-config access, unauth SPL search	10.6.1 / 10.4.5 / 10.2.9 / 10.0.12 / 9.4.17	not reported
Ruby (Ruby2Shell + 6)	heap overflow in String case conversion	4.0.10 / 3.4.13 / 3.3.14	PoCs; no attacks
PHP	18 CVEs incl. FPM smuggling (9.2), phpAfterShell	8.5.13 / 8.4.28 / 8.3.37 / 8.2.36	not reported
GnuPG GPGME	double free from a crafted OpenPGP key	GPGME 2.3.0+; rebuild bundled copies	not reported
Linux KVM (AMD, nested virt)	guest reads host memory, CVE-2026-99312	upstream kernel; distros pending	not reported
WhatsApp (Android)	CVE-2026-23871, IP leak via ad reply (3.5)	2.26.17.4	suspected in scams
Windows “FastUnlock”	lock-screen bypass, physical access	no patch	not reported

Table 6 · Sources: SonicWall [57], The Hacker News [58, 62, 63, 64, 65], SecurityWeek [59], ruby-lang.org [60], php.net [61].

SONICWALL GEN 6: UNTIL IT IS GONE

1. No WAN management (HTTPS, SSH, SNMP).
2. SSL VPN off, or limited to known source addresses.
3. MFA on remote and admin accounts; reset local passwords.
4. Watch logs for unusual logins and config changes.

SonicWall says these steps do “not make Gen 6 secure”. Replacement is the fix. [57]

RUNTIMES: REBUILD, DON'T JUST UPDATE

- Ruby2Shell and the PHP bugs live in the interpreter; gem or app updates do not touch them.
- Rebuild base images, redeploy and restart long-running workers and PHP-FPM pools.
- GPGME: applications that bundle their own copy need their own updates.
- KVM hosts: update the host kernel or disable nested virtualization on AMD. [63]

TWO DETAILS WORTH A SECOND LOOK

- Splunk CVE-2026-76536 applies when the clustering shared secret is empty: set one even after patching. Enterprise Security and SOAR fixes are 8.7.0 and 8.8.0. [59]
- F5's six critical BIG-IP flaws only bite with specific iRule commands or APM policies, and fixes are engineering hotfixes: check your configuration before scheduling. [16]
- PHP says its critical bugs need “non-default or uncommon configurations”; patch anyway, but prioritise PHP-FPM behind proxies. [61]

Who was behind it, and who got caught

Attribution below is quoted as each researcher stated it. Confidence levels matter: “suspected” and “moderate confidence” are not proof.

ARMORY CASTLE (China)

GTIG: “suspected PRC-nexus espionage actor ARMORY CASTLE (formerly tracked as UNC5221)”. vCenter zero-day since September, entry through BeyondTrust. See pages 5–6. [5]

Cold Relic (Russia)

GTIG described the group (formerly COLDRIVER) taking over one firm's Google Workspace, then posing as its staff to breach a second. Persistence via passkeys and rogue MFA devices that survived password resets. [67]

EggStreme (China-nexus)

Bitdefender: rebuilt after exposure, with passive agents listening on TCP 5060 behind a “Core Networking - SIP” firewall rule. Philippine government targeting, high confidence. [66]

North Korea-linked lures

MIDNIGHT NEPTUNE backdoored Claude Code settings (GTIG). Stormshield's Trigram fake-recruiter campaign shows “strong similarities” to North Korean sets, with no firm attribution. [20]

BO Team (Ukrainian origin)

Kaspersky: Log4Shell in vCenter 7.0.3 led to a Russian developer's code-signing server; no malicious signed release confirmed. Report dated 5 Nov. [68]

ROMULUS

ClickFix lures, including ChatGPT Custom GPTs, deliver the CNCMachineRMS RAT with DNS-over-HTTPS command and control. No actor named. [69]

LAW ENFORCEMENT

- Roman Khlynovskiy, a Kazakh national, was extradited from Italy and appeared in court in Knoxville on 16 Nov. Prosecutors allege he belonged to the “8-Digits Team” behind INC and Lynx attacks; they allege $500M in ransom demands. These are allegations. [50]
- SecurityWeek briefly reports four arrests in Ukraine with the FBI; we could not confirm details. [43]

POLICY

- Project Zero: “Full 90” disclosure from 13 Nov, Full 60 from February 2027, Full 30 from January 2028. [26]
- BIS interim final rule (16 Nov) on remote access to advanced chips through third-country data centres. [70]
- National Cyber Director Sean Cairncross is out; Pentagon CIO Kirsten Davies is acting. [51]
- CISA's KEV entries now cite BOD 26-04 and forensics-triage requirements. [1]

READING GOOGLE'S NEW ACTOR NAMES

SUFFIX	MEANS
CASTLE	China
RELIC	Russia
NEPTUNE	North Korea
ION	Iran
COMET	financially motivated crime

GTIG introduced the scheme in July 2026, so older reports use names like UNC5221 and COLDRIVER.

EVICTION IS MORE THAN A PASSWORD RESET

- Cold Relic kept access through passkeys and MFA devices it registered itself.
- ARMORY CASTLE stole vCenter's SAML signing key to forge logins.
- agent-framework stole OIDC and managed-identity tokens.
- On compromise: revoke sessions, remove unknown passkeys and MFA devices, audit OAuth grants, rotate signing certificates and federated credentials.

Your work list for next week

Ordered by urgency. Federal KEV deadlines are a useful clock even if you are not a US agency.

WHEN	TEAM	ACTION	SEE
BY 23 NOV	Virtualization	Patch vCenter (8.0 U3m / 9.0.2.0200 / 9.1.1.0200; VCF 5.2.5); TCP 2012 to vCenter peers only.	p.05–06
BY 23 NOV	UC / network	Expressway clusters to X15.5.20; TCP 4372 to cluster peers only; grep logs for wombat@127.0.0.1.	p.07
BY 23 NOV	Apps	Roller to 6.1.6+ or disable XML-RPC; apply SAP's Nov 2025 fix for CVE-2025-42884.	p.04, 08
THIS WEEK	SOC / IR	Hunt GTIG's vCenter indicators; if found, rotate the STS signing certificate and treat AD as exposed.	p.06
THIS WEEK	Dev / CI	Search for agent-framework 1.26.1/1.26.2; rebuild and rotate tokens. Review agent config files in repos.	p.10–11
THIS WEEK	AI platform	Authenticate or unexpose LiteLLM, Langflow, Ollama, MONAI Label; spend alerts on model keys.	p.10
THIS WEEK	Platform	Puppet, Splunk, Ruby, PHP, GPGME, N-central HF3 (with agents and probes).	p.08, 15
THIS MONTH	Network	Replace SonicWall Gen 6; until then no WAN management and restricted SSL VPN.	p.15
THIS MONTH	OT / facilities	Take refrigeration controllers and PLC web UIs off the internet; list end-of-life devices.	p.14
THIS MONTH	Third-party risk	Inventory vendor keys and data shares; retire keys from finished projects.	p.11

ONE-PAGE HUNT SHEET

vCenter	sps-*@vsphere.local · SUID on /bin/env · /tmp/123, /tmp/sss, /tmp/dbr · SSH banner pulsesecure_23345
Expressway	wombat@127.0.0.1 in erlang.log · .py under /mnt/harddisk/i####/ · 66.179.31[.]32, 18.130.47[.]116
PyPI	agent_framework_meta.pth · af_runtime_diag.pth · webhook[.]site exfil
AI servers	sitecustomize.py you did not write · MONAI: 142[.]4.98.145, 142[.]4.107.34
Repos	.claude/settings.json changes · tokens named like Copilot

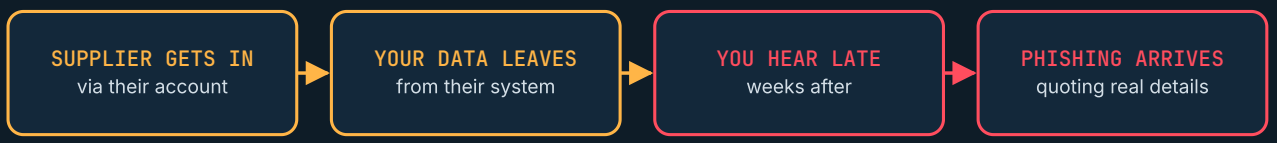
BEFORE YOU CLOSE A TICKET

- Version numbers match the vendor's fixed builds on every node, including DR and lab.
- Management and cluster ports unreachable from user networks.
- Rotated secrets are actually revoked, not just replaced.
- Every exception has an owner and a date.

Indicators are copied from the cited reports (GTIG, F6 via SecurityWeek, Wiz, Amazon) and were not tested by MAG212. Check them against your own logs, and test only systems you are authorised to assess.

When the breach is at someone else's company

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



Your security now depends on people you never hired.

Ask what each supplier holds, how they would tell you, and how fast.

This week: Uber, JPMorgan, Visa, Mastercard, Infoblox and 40+ credit unions learned it the hard way

Figure 6 · How supplier breaches reach customers. Conceptual illustration, MAG212 CYBER, based on this week's cases [33, 36, 38].

FOR EVERY EMPLOYEE

- A message that mentions a real order, booking or account number is not proof it is genuine.
- Call back on a number you already have, not one in the message.
- Never paste a "fix" command a website or chat tells you to run (ClickFix).
- Report unexpected MFA prompts; never approve one you did not start.

FOR ADMINISTRATORS

- Keep a list of every supplier key, token and data feed, with an owner and an end date.
- Prefer short-lived, scoped credentials for vendors and AI tools.
- Log and alert on supplier accounts like your own staff's.
- Patching does not evict an intruder: rotate keys, certificates and sessions too.

FOR BUSINESS LEADERS

- Contracts should say how fast a supplier must tell you about a breach. Wellington IT's customers waited six weeks.
- Ask for one page per critical supplier: what they hold, where, and who can reach it.
- Budget for the AI tools your teams already use; ungoverned keys are how this week's AI attacks were paid for.

THREE QUESTIONS FOR YOUR NEXT MEETING

1. Which suppliers hold our customers' data, and when did we last check their access?
2. Which vendor keys or accounts belong to projects that have ended?
3. If a supplier told us of a breach today, who would decide what we tell customers?

Sources (1 of 2)

[1] CISA (GitHub mirror) · 20 Nov 2026 · Known Exploited Vulnerabilities catalog, version 2026.11.20

[2] The Hacker News · 21 Nov 2026 · Hackers exploit critical VMware, Cisco flaws; CISA adds four to KEV

[3] The Hacker News · 19 Nov 2026 · CISA warns of 4 exploited flaws (Axis, REDCap, LiteLLM, Synology)

[4] Broadcom · 19–20 Nov 2026 · VMSA-2026-0009.1: vCenter Server, Cloud Foundation and Tools

[5] Google GTIG / Mandiant · 19 Nov 2026 · ARMORY CASTLE exploits vSphere zero-day

[6] Rapid7 · 19 Nov 2026 · ETR: CVE-2026-123890 critical authentication bypass in VMware vCenter

[7] Ostorlab · 19 Nov 2026 · VMware vCenter authentication bypass CVE-2026-123890

[8] Mandiant (GitHub) · accessed 21 Nov 2026 · vcsa-hardening-tool

[9] Cisco · 21 Oct 2026, checked 21 Nov · cisco-sa-vcs-static-cred-hr7EWZ8t (v1.0)

[10] SecurityWeek · 19 Nov 2026 · Hackers exploit Cisco Expressway vulnerability soon after PoC release

[11] Ostorlab · 19 Nov 2026 · Cisco Expressway root RCE CVE-2026-76466

[12] BleepingComputer · 18 Nov 2026 · Apache warns of Roller RCE vulnerability exploited in attacks

[13] The Hacker News · 17 Nov 2026 · Hackers exploiting critical Puppet RCE

[14] SecurityWeek · 19 Nov 2026 · Java4Shell exploitation attempts begin as vendors rush out advisories

[15] SecurityWeek · 19 Nov 2026 · F5 patches critical nginx2root flaws as PoC exploits go public

[16] The Hacker News · 18 Nov 2026 · F5 warns of 6 critical BIG-IP flaws

[17] The Hacker News · 19 Nov 2026 · Drupal patches critical installer flaw

[18] Amazon Threat Intelligence · 20 Nov 2026 · Chinese-nexus actors' Cairn AI agents found a zero-day on their own

[19] The Hacker News · 21 Nov 2026 · Attackers' AI agents found zero-day in MONAI Label

[20] Google GTIG · 16 Nov 2026 · AI Threat Tracker: agentic threat activity crosses a significant threshold

[21] Amazon Threat Intelligence · 13 Nov 2026 · Threat actors running cybercrime campaigns with ARTEX AI agents

[22] The Record · 13 Nov 2026 · FBI FLASH alert on ARTEX AI tool

[23] Barracuda · 11 Nov 2026 · Anatomy of a machine-speed intrusion

[24] Help Net Security · 20 Nov 2026 · European Commission: AI-generated cyberattack used publicly available tool

[25] SecurityWeek · 20 Nov 2026 · European Commission confirms AI-assisted cyberattack disrupted services

[26] Google Project Zero · 13 Nov 2026 · Disclosure policy update: Full 90

[27] The Hacker News · 21 Nov 2026 · A single malicious webpage let attackers hijack Meta's Muse agent

[28] The Hacker News · 21 Nov 2026 · Signal blocks AI agents from reading chats

[29] Wiz · 17–18 Nov 2026 · Malicious version of Microsoft's agent-framework published to PyPI

[30] Cloud Security Alliance · 19 Nov 2026 · Research note: Microsoft agent-framework PyPI compromise

[31] The Register · 18 Nov 2026 · Microsoft makes repositories private amid PyPI compromise

[32] Unit 42 · 17 Nov 2026 · OPTIMJACK supply chain attack

[33] SecurityWeek · 16 Nov 2026 · Uber data breach impacts 150,000 people

[34] The Hacker News · Nov 2026 · Stolen Fireworks AI key led to Cursor compromise

[35] TechRadar · 17 Nov 2026 · Infoblox confirms company and customer data exposed in SharePoint breach

[36] SecurityWeek · 20 Nov 2026 · JPMorgan, Visa, Mastercard cite third-party incidents amid data leak

[37] Valley News Live · 19 Nov 2026 · Expedia investigates cyberattack after hackers claim theft of nearly 1 billion records

[38] The Record · 20 Nov 2026 · Dozens of credit unions hit by supplier breach

[39] SEC EDGAR · 18 Nov 2026 · SBC Medical Group Holdings 8-K, Exhibit 99.1

[40] Security Affairs · 15 Nov 2026 · Data breach at La Poste subsidiary Maileva affects 22 million people

Sources (2 of 2)

[41] Help Net Security · 20 Nov 2026 · Transport for London Oyster photocard data breach

[42] BleepingComputer · 17 Nov 2026 · Japan takes Fugaku supercomputer offline after cyberattack

[43] SecurityWeek · 20 Nov 2026 · In Other News: Norwegian energy firm, supercomputer hack, Rakuten Securities

[44] Equinor · 17–20 Nov 2026 · Newsroom: cyber-attack updates

[45] The Hacker News · 19–20 Nov 2026 · N-able confirms hackers accessed cloud server

[46] BleepingComputer · 19 Nov 2026 · Nvidia investigating Gentlemen ransomware breach claims

[47] Ipsos · 17 Nov 2026 · Ipsos announces it filed a complaint regarding a breach of one of its internal systems

[48] Coles Group · 16 Nov 2026 · Updates: cyber security incident

[49] The Record · 20 Nov 2026 · West Virginia Legislature hit by cyberattack

[50] The Record · 17 Nov 2026 · Kazakh suspect extradited on 8-Digits Team ransomware charges

[51] The Record · 20 Nov 2026 · Sean Cairncross out as National Cyber Director

[52] SecurityWeek · 16 Nov 2026 · Hackers probe newly disclosed flaws in Copeland refrigeration controllers

[53] The Hacker News · 16 Nov 2026 · Weekly recap (Danfoss AK-SM 800A disclosure)

[54] TheHackerWire · 21 Nov 2026 · CVE-2026-96805: Elecbrakes wireless trailer brake BLE hijack

[55] Security Boulevard · 20 Nov 2026 · Daily OT security news, November 20, 2026

[56] Huntress · 13 Nov 2026 · GeoVision camera software XMRig cryptominer

[57] SonicWall · 18 Nov 2026 · Product advisory: Retire unsupported Gen 6 firewalls

[58] The Hacker News · 17 Nov 2026 · N-able patches 17 N-central flaws (2026.4 HF3)

[59] SecurityWeek · 19 Nov 2026 · Splunk patches nearly 140 flaws across three core products

[60] ruby-lang.org · 18 Nov 2026 · Multiple vulnerabilities in Regexp and String

[61] PHP · 19 Nov 2026 · PHP 8 ChangeLog (8.5.13, 8.4.28, 8.3.37, 8.2.36)

[62] The Hacker News · 21 Nov 2026 · GnuPG warns critical GPGME flaw

[63] The Hacker News · 20 Nov 2026 · New Linux KVM flaw CVE-2026-99312

[64] The Hacker News · 20 Nov 2026 · WhatsApp patches 3 security flaws

[65] The Hacker News · 20 Nov 2026 · New unpatched Windows 0-day FastUnlock

[66] Bitdefender · 18 Nov 2026 · EggStreme malware revises architecture and infrastructure

[67] The Hacker News · 18 Nov 2026 · Russian Cold Relic hackers use stolen identities

[68] The Hacker News · 16 Nov 2026 · BO Team exploits Log4Shell in VMware to reach code-signing server

[69] The Hacker News · 20 Nov 2026 · ROMULUS ClickFix attacks deliver RAT

[70] US BIS · 16 Nov 2026 · Interim final rule: remote access to advanced semiconductors

HOW WE VERIFIED THIS ISSUE

- Primary sources read: CISA's KEV catalog data (official GitHub mirror, v2026.11.20), Broadcom's VMSA, GTIG/Mandiant, Amazon Threat Intelligence, Cisco's advisory, Wiz, SonicWall, SBC's SEC filing, Equinor's newsroom, ruby-lang.org and php.net.
- cisa.gov itself was unreachable: KEV dates come from the catalog data; ICS advisory details come from secondary sources and are labelled.
- F6's Expressway report, Politico's Commission story and Microsoft's root cause were not available; those points are labelled as reported or unconfirmed.
- Items published 11–13 November (FBI ARTEX FLASH, Amazon ARTEX report, Barracuda, Project Zero) are dated as such. No command or indicator was tested 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

Weekly · 21 November 2026
Understand the threat. Build the defense.