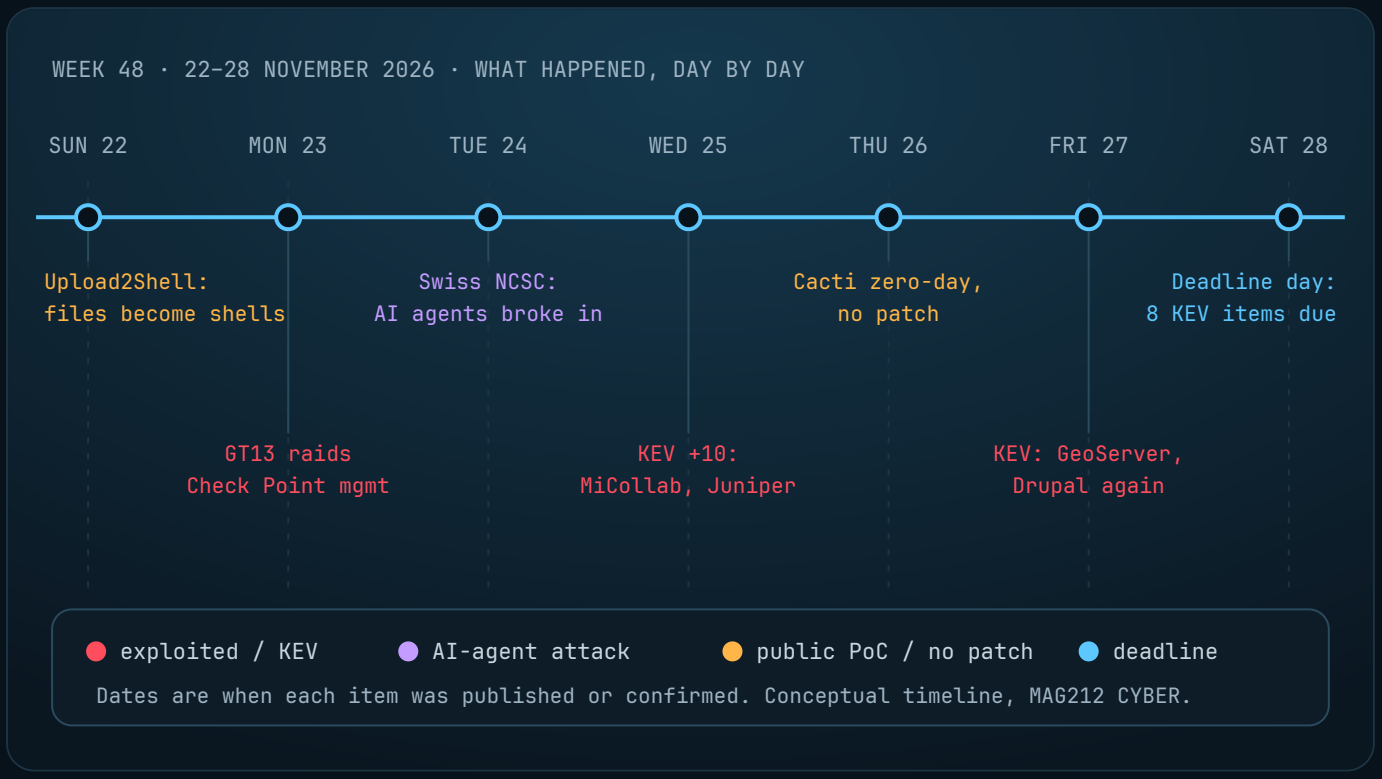
# MAG212 CYBER

WEEKLY

Saturday, 28 November 2026

WEEK OF 22–28 NOV · CUTOFF 8:00 AM PT




THE WEEK IN CYBER · 22–28 NOVEMBER

# Old doors, new speed

Switzerland confirmed attacks run by AI agents, and the way in was a weak password or a known flaw. Attackers went for the consoles that manage firewalls, routers and phone systems. Two software vendors lost production data through a developer's credentials. Here is what is confirmed, and what to fix first.


04 KEV board: 18 additions, 8 due today

05 AI agents broke in, through old doors

07 The consoles that run everything

08 MiCollab: phone server to domain in 32 min

10 One developer account, wide reach

11 Cacti zero-day, nginx2root, PHP, Ghostscript


**18**
flaws added to CISA KEV, 23–27 Nov

**4 OF 5**
Swiss AI-agent attacks that succeeded

**32 MIN**
MiCollab: first request to domain controller

**24**
Check Point managers used by GT13

# What mattered this week

Developments published or confirmed 22–28 November 2026; earlier items are dated as such.

### Agents, through old doors

Switzerland's NCSC confirmed five attacks run with AI agents; four succeeded. The way in was a guessed password or a known flaw. Italy's CSIRT reports the same pattern. [5][6][7]

### The consoles that run everything

GT13 used 24 Check Point management servers; a Juniper Conductor flaw is exploited; Broadcom fixed a 9.8 vCenter login bypass, not yet exploited. [13][15][12]

### Servers hit before or right after the fix

Five MiCollab flaws were used before Mitel's patch. Drupal's installer was exploited twice in a week. GeoServer joined KEV. [20][23][1]

### One developer account, wide reach

An employee's GitHub account gave access to 1Password's backend; a development key reached Todoist production in a day; PolinRider spread through developers' repos. [26][28][30]

## THE THREE PRIORITY ACTIONS

1. **Clear this weekend's KEV list, then hunt.**
   Due today: Juniper Conductor, Xen Orchestra, MiCollab. Due Monday: Drupal (run update.php) and GeoServer. Patched is not the same as clean. [1][23][25]
2. **Put MFA or passkeys on every internet-facing login.**
   Webmail, VPN and admin portals first; patch exposed systems within 24 hours, as the Swiss NCSC asks. [5]
3. **Treat developer and CI credentials as production credentials.**
   Phishing-resistant MFA, short-lived tokens, reviewed workflow changes, alerts on new admin accounts. [26][28]

## STATUS AT A GLANCE

| ISSUE | STATUS | ACT BY |
|---|---|---|
| Mitel MiCollab (5 CVEs) | EXPLOITED BEFORE FIX · KEV | 28 Nov / 9 Dec |
| Juniper Conductor CVE-2026-103406 | EXPLOITED · KEV | 28 Nov |
| Drupal CVE-2026-136716 | EXPLOITED · KEV | 30 Nov |
| GeoServer CVE-2026-120705 / 129243 | EXPLOITED · KEV | 30 Nov |
| Cacti 1.2.31 chain (no CVE) | PoC PUBLIC · NO PATCH | disable guest |

## CONTENTS


03 Day by day
04 KEV board
05 AI agents
06 Defending
07 Management consoles
08 MiCollab
09 Drupal; GeoServer
10 Developer accounts
11 Web servers
12 Cloud and devices
13 Incidents
14 Action Desk
15 Awareness
16 Sources

# Seven days in eight lines

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

| | | |
|---|---|---|
| SUN 22 | 🟡 | N-able discloses a Mail Assure SSRF, CVE-2026-134624, after its cloud-server breach. The Hacker News covers the Upload2Shell Ghostscript research. [47][39] |
| MON 23 | 🔴 | GreyNoise details GT13's Check Point campaign. NSM updates its Azure API Management advisory. KEV adds MONAI Label and Mail Assure. The Commission confirms an EU Academy data breach. [13][41][4][48] |
| TUE 24 | 🟣 | Swiss NCSC confirms its first AI-agent attacks. Broadcom ships VMSA-2026-0011 (23 CVEs). KEV adds Drupal, Optimizely and Idunno. Check Point Research names Volant Manticore. [5][12][1][45] |
| TUE 24 | 🟡 | Juniper's bulletin now reports exploitation. Todoist publishes its incident timeline. AP source: an unclassified CIA system was breached. [15][28][50] |
| WED 25 | 🔴 | Drupal SA-CORE-2026-019: the first fix missed some sites. 1Password discloses a GitHub-account breach. KEV adds 10: MiCollab ×5, Juniper, Xen Orchestra, Danfoss ×3. [23][26][2] |
| THU 26 | 🔴 | Accenture: MiCollab flaws were used before Mitel's fix. PolinRider found in 7,600+ repos. The Cacti 4HTTP2ROOT chain is published with no patch. FIFA confirms an attack. [20][30][34][53] |
| FRI 27 | 🔴 | KEV adds GeoServer CVE-2026-120705 and CVE-2026-129243, and Drupal CVE-2026-136716, all due 30 November. [1] |
| SAT 28 | 🔵 | Federal deadline for eight KEV entries: Juniper, Xen Orchestra, four MiCollab flaws and two Danfoss flaws. [1] |

### PUBLISHED JUST BEFORE THE WEEK, STILL LANDING

- 18 Nov: nginx.org fixes five nginx2root memory-corruption flaws. Rapid7 counts 7,675 Ollama AI servers open without login in its sample. [32][46]
- 19 Nov: PHP fixes phpAfterShell, CVE-2026-126714. Microsoft closes the Azure API Management access path. [36][42]
- 20 Nov: Amazon describes Cairn AI agents finding a MONAI Label zero-day. GL.iNet reports its GoodCloud compromise. [9][43]

CATALOG 2026.11.27 · 1,808 ENTRIES | 18 ADDITIONS 23–27 NOV | 8 DUE TODAY

# 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 |
|---|---|---|---|---|
| 27 Nov | 30 Nov | CVE-2026-120705, -129243 | OSGeo GeoServer | File read/SSRF, role bypass; chain to RCE |
| 27 Nov | 30 Nov | CVE-2026-136716 | Drupal core | Installer takeover, odd install states (SA-019) |
| 25 Nov | 28 Nov | CVE-2026-103406 | Juniper Session Smart | Command injection as root, no login |
| 25 Nov | 28 Nov | CVE-2026-133469 | Vates Xen Orchestra | Authentication bypass to admin rights |
| 25 Nov | 28 Nov / 9 Dec | CVE-2026-133323 +4 | Mitel MiCollab (AWV) | Used before the 16 Nov fix (Accenture) |
| 25 Nov | 28 Nov / 9 Dec | CVE-2023-25914, -25915, CVE-2025-41450 | Danfoss AK-SM 800A | Old flaws on a long-lived controller |
| 24 Nov | 27 Nov | CVE-2026-132165 | Drupal core | Installer reinstall; exploited from 19 Nov |
| 24 Nov | 27 Nov | CVE-2026-132224 | Optimizely Web Exp. | Signup flow allowed user impersonation |
| 24 Nov | 27 Nov | CVE-2026-131914 | Idunno AntiCsrf | Deserialization, unauthenticated RCE |
| 23 Nov | 26 Nov | CVE-2026-133968 | MONAI Label | Found by AI agents (Amazon); 0.8.6 |
| 23 Nov | 26 Nov | CVE-2026-134624 | N-able Mail Assure | SSRF in LDAP sync check |

Table 1 · CISA KEV additions 23–27 November, from the official catalog data (GitHub mirror, version 2026.11.27) [1] and CISA's 25 November alert [2]. CISA's 27 November alert page did not load for us [3].

## WHAT CHANGED

- Three-day deadlines are now normal for exploited, internet-facing flaws. Entries cite CISA's BOD 26-04 and its forensics-triage requirements. [1]
- Drupal appears twice: the 24 Nov entry for the first installer flaw, and the 27 Nov entry for sites the first fix missed. [23][1]
- GeoServer fixed these in October releases; its project page does not say they are exploited. CISA does. [25][1]

## HOW TO USE THIS BOARD

1. Find each product in your inventory, including lab and DR copies.
2. Patch internet-facing management and collaboration servers first: Conductor, MiCollab, Xen Orchestra, GeoServer, Drupal.
3. Where you cannot patch by the due date, remove exposure and log the exception.
4. Hunt on every listed system exposed before you patched: a patched system may already be compromised.
5. Re-check the catalog on weekdays.

## DUE NEXT

30 Nov: GeoServer CVE-2026-120705 and CVE-2026-129243; Drupal CVE-2026-136716 · 1 Dec: Puppet Enterprise CVE-2026-115731 · 2 Dec: LiteLLM CVE-2026-40217 · 9 Dec: Danfoss CVE-2025-41450, MiCollab CVE-2026-133311. Not in KEV at our check: Cacti, nginx2root, phpAfterShell. [1]

SWISS NCSC | CSIRT ITALIA | UK NCSC | AMAZON · GREYNOISE · ACCENTURE

# AI agents broke in, through old doors

This was the week national CERTs confirmed attacks run by AI agents. None needed a new technique: weak passwords and known flaws were enough.

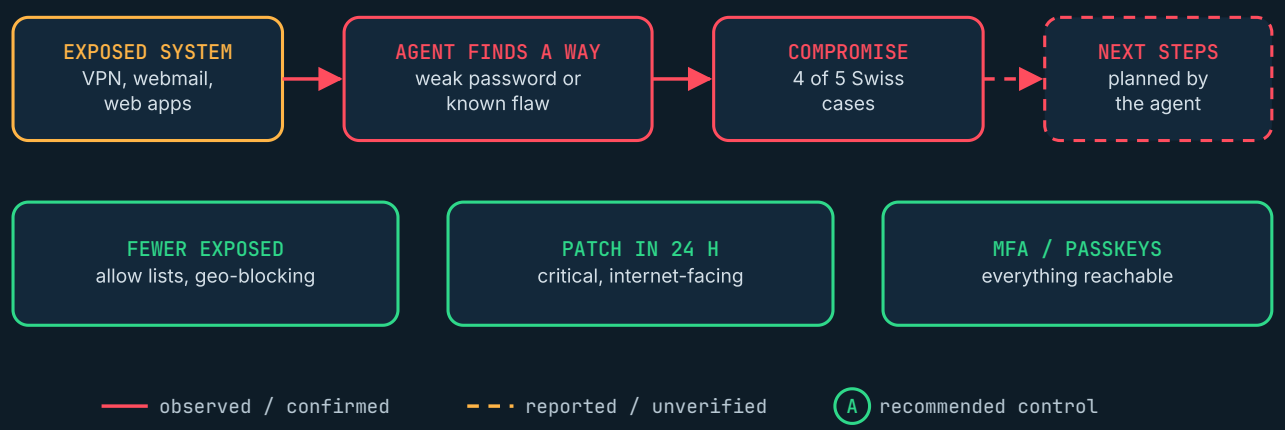



Figure 1 · The pattern the Swiss NCSC describes [5]. Green boxes are its recommended defences. MAG212 CYBER diagram.

| WHO REPORTED | WHAT THEY SAW | AI ROLE |
|---|---|---|
| Swiss NCSC, 24 Nov | 5 confirmed attacks, 4 succeeded; 3 on infrastructure operators, 2 succeeded, no major disruption | CONFIRMED |
| CSIRT Italia, 25 Nov | Agents compromised many systems within hours and wrote code on the fly to evade endpoint tools | REPORTED |
| Amazon, 20 Nov | Cairn agents found and exploited a MONAI Label zero-day in about 11 minutes; 148 actions over 16 hours failed against Redis | OBSERVED, HIGH CONF. |
| GreyNoise, 23 Nov | GT13 tasks across 24 Check Point managers, with automated checks and output written in IP order | SUSPECTED |
| Accenture, Nov | MiCollab attacker's server contacted two commercial AI services in step with the exploit | MODERATE CONF. |

Table 2 · Sources: Swiss NCSC and The Hacker News [5, 6], BleepingComputer [7], Amazon [9], GreyNoise [13], Accenture [20]. Confidence labels are each source's own.

### WHAT AN AGENT DOES

The NCSC calls them agentic offensive frameworks: they look for weaknesses, pick tools, judge the result and plan the next step, switching methods when blocked. It says publicly reachable ones such as ARTEX and CyberStrikeAI have almost doubled since October, without saying these were used in the Swiss cases. [5][6]

### WHAT IS NOT KNOWN

- Victims, attackers and tools in the Swiss and Italian cases.
- Which flaws were used in each case.
- Whether GT13 and the MiCollab attacker used AI; both are assessments, not proof.

**STATUS** Confirmed by national CERTs; the UK NCSC reports a marked rise in AI-assisted attacks since September. [8][6]

# Defending at machine speed

The Swiss NCSC's six measures, to be put in place “without delay”. None is new; the deadline is.

| # | NCSC MEASURE | WHAT IT MEANS IN PRACTICE |
|---|---|---|
| 1 | Limit exposed systems | Allow lists or geo-blocking on admin portals, VPN and remote access |
| 2 | Patch within 24 hours | Critical updates on internet-facing systems, the day they ship |
| 3 | MFA or passkeys, everywhere | Every internal resource reachable from outside: webmail, VPN, portals |
| 4 | Least privilege | Service and user accounts get only the access they need |
| 5 | Watch behaviour and volume | Alert on unusual identity activity and data leaving in bulk |
| 6 | Test regularly | Penetration tests, in-house or external |

Table 3 · From the Swiss NCSC advisory [5]. The right-hand column is MAG212's plain-language reading.

Windows · PowerShell · RSAT ActiveDirectory module

domain user READ-ONLY

NOT TESTED BY MAG212

find weak spots

```
Get-ADUser -Filter 'PasswordNeverExpires -eq $true' | Select-Object SamAccountName
```

Lists accounts whose passwords never expire, a common home for weak, old passwords. Review the list; it changes nothing. Not tested by MAG212.

### AUTOMATE THE FIRST RESPONSE

Amazon's advice after the Cairn campaign: agents work around the clock, so let high-confidence detections trigger automatic containment, with people supervising outcomes rather than approving every step. [9]

### WHERE TO START THIS WEEK

1. List every internet-facing system and its owner.
2. Turn on MFA where it is missing.
3. Agree who can approve an emergency patch at night or at a weekend.
4. Alert on new admin accounts and bulk exports.

### FOR LEADERS

- A 24-hour patch target needs staff, testing and authority to restart systems.
- Fund MFA and attack-surface monitoring before tools that promise AI defence.

MAG212 analysis.

### HOW TO KNOW YOU ARE READY

- No internet-facing login without MFA.
- Critical patches applied within a day, and measured.
- Alerts fire on bulk data movement and new privileged accounts.

CHECK POINT · GT13 | JUNIPER CONDUCTOR | XEN ORCHESTRA | VMSA-2026-0011

# The consoles that run everything

A firewall manager, a router conductor or a hypervisor console holds the keys to every device below it. Attackers went for all three this week.

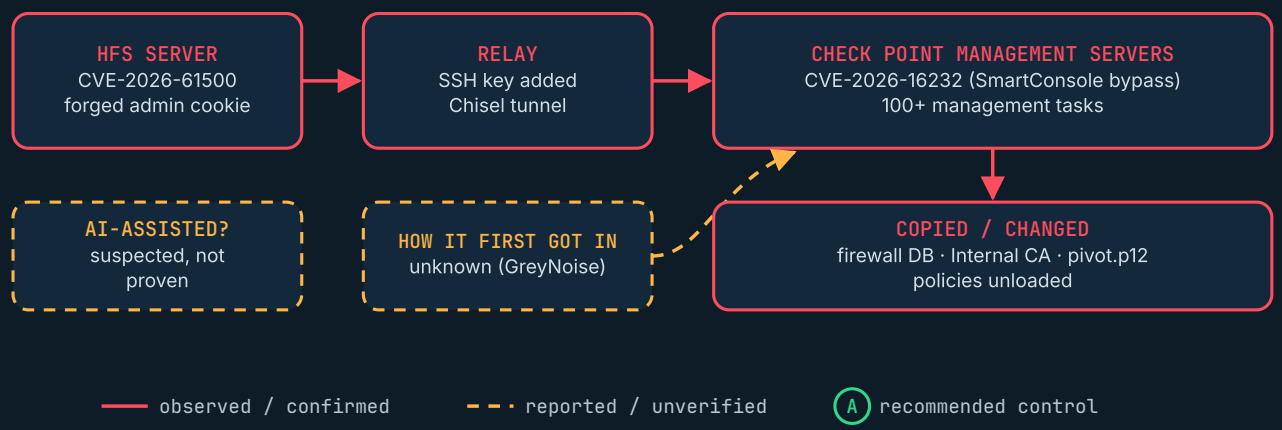



Figure 2 · GT13's path as GreyNoise reconstructed it. The first route to the Check Point servers is unknown; AI use is GreyNoise's suspicion [13]. MAG212 CYBER diagram.

| CONSOLE | ISSUE | STATUS | DO |
|---|---|---|---|
| Check Point Security Mgmt | CVE-2026-16232 auth bypass, used by GT13 on 24 servers | USED IN ATTACKS | Confirm July fix; review tasks, CA, /etc/ld.so.preload |
| Juniper Session Smart Conductor | CVE-2026-103406, Salt minion ID command injection as root (9.8) | EXPLOITED · KEV 28 NOV | 7.0.5 / 7.1.7 / 7.2.3; admin-network only |
| Xen Orchestra | CVE-2026-133469, crafted token gives admin; can lead to root on hosts | EXPLOITED · KEV 28 NOV | 6.10.1 or 6.9.2 |
| VMware vCenter | CVE-2026-123903 vmdir login bypass (9.8), in VMSA-2026-0011 | NOT EXPLOITED (24 NOV) | 9.1.2 / 9.0.2.0300 / 8.0 U3m |
| VMware ESX | CVE-2026-123910 and -123911, I/O filter service (9.8) | NOT EXPLOITED (24 NOV) | Builds per VMSA-2026-0011 |

Table 4 · Sources: GreyNoise [13], SecurityWeek and eSecurity Planet on Juniper [15, 16], The Hacker News on Xen Orchestra [18], Broadcom [12], CISA KEV [1]. Juniper's bulletin did not load for us [17].

### GT13 IN ONE PARAGRAPH

Between 2 October and 2 November an unknown actor reached at least 22 organisations in 17 countries and ran more than 100 tasks on Check Point management servers, copying firewall databases and the Internal CA and minting a certificate called pivot.p12. GreyNoise expects the intrusion is ongoing. We had found no Check Point statement as of 25 November. [13][14]

### WHAT TO DO WITH ANY CONSOLE

1. Reachable only from an admin network or jump host.
2. Patched first, before the devices it manages.
3. Logs and an image kept before you upgrade.
4. Look back: new accounts, tasks, certificates, pushed configs.

MITEL MISA-2026-0012 | ACCENTURE APEX LABS | 5 CVEs ON KEV

# MiCollab: from phone server to domain in 32 minutes

Attackers used five flaws before Mitel's 16 November patch, then went for Active Directory, backups and databases.

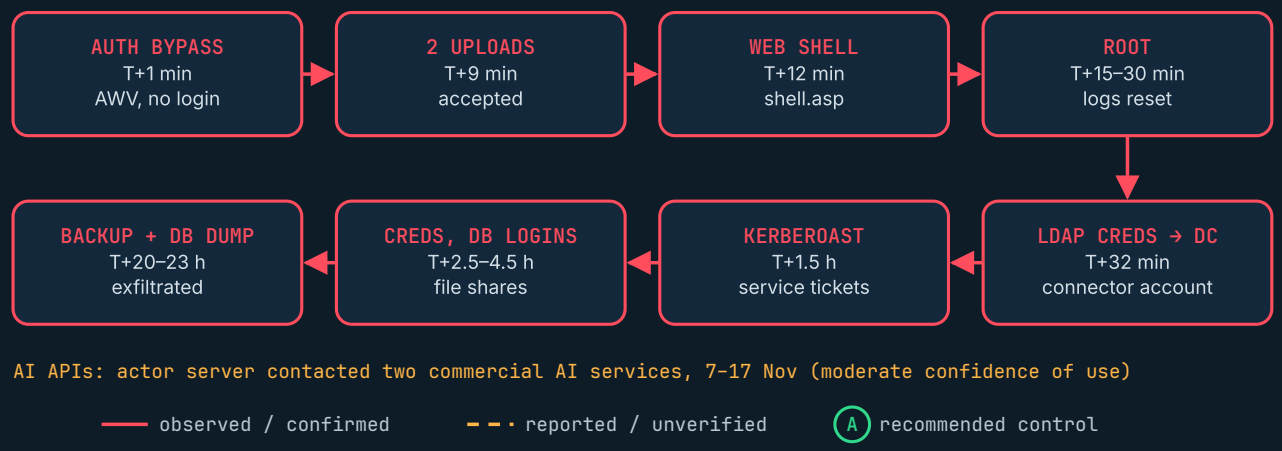



Figure 3 · One intrusion as Accenture APEX Labs timed it, from the first request [20]. MAG212 CYBER diagram.

| CVE | WHAT (AWV COMPONENT) | CVSS | KEV DUE |
|---|---|---|---|
| CVE-2026-133323 | Blind command injection | 10.0 | 28 Nov |
| CVE-2026-133303 | XML injection, pre-staged content | 9.0 | 28 Nov |
| CVE-2026-133311 | Sensitive information access | 5.9 | 9 Dec |
| CVE-2026-133275 | Arbitrary file upload | 5.3 | 28 Nov |
| CVE-2026-133324 | Authentication bypass | 5.3 | 28 Nov |

Table 5 · Mitel MISA-2026-0012 rev 2.0 [19]; CISA KEV [1]. Fix: KB000129195 on 10.3.0.18, or a later release.

Mitel's advisory does not mention attacks. Accenture found a web shell at one victim before 23:00 UTC on 15 November, and a second server talking to the same attacker host since 9 November. It suspects data-theft extortion and names no group. [19][20]

### CONTAIN, IN ORDER

1. Block external access to AWV.
2. Image the server, then patch.
3. Reset the LDAP connector and Kerberoastable service accounts.
4. Patch older MiCollab flaws on lagging servers.

### HUNT (ACCENTURE)

| WHERE | LOOK FOR |
|---|---|
| Web root | New files under /pictures/ (shell.asp, shell.jsp) |
| Web logs | POSTs to /awcuser/cgi-bin/ then new /pictures/ files; curl/8.14.1 |
| /tmp | roast*.py, mkccache.py, testcreds*.py, relay*.py, *.tgz |
| Network | HTTP PUT to /bkup/; 204.76.203[.]204 and .216; trycloudflare, ipify |
| Identity | LDAP connector logging on to many DCs; bursts of RC4 Kerberos tickets |

From Accenture [20]. Assume local logs were edited; a sudden drop in log size is itself a signal.

# Drupal's installer, twice; GeoServer on KEV

Two open-source servers where the fix existed before the attacks, and where a patched site may already be compromised.

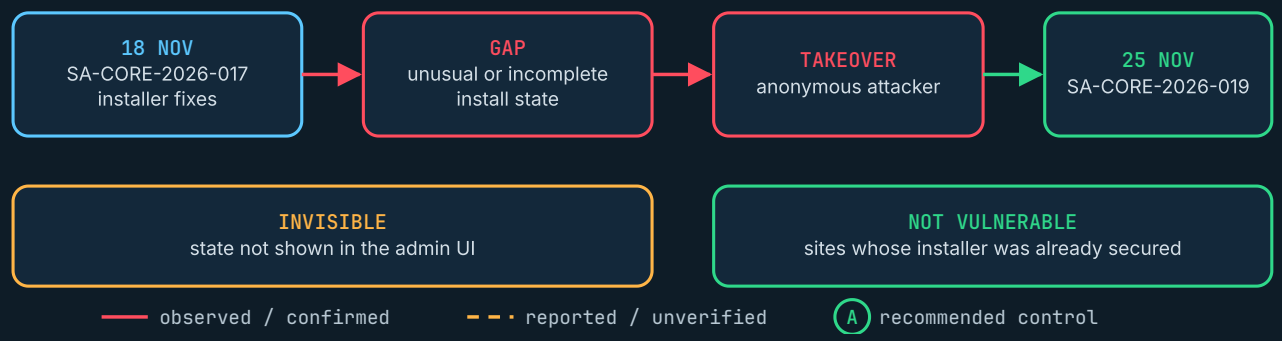



Figure 4 · What changed between Drupal's two advisories [23, 22]. MAG212 CYBER diagram.

| ADVISORY | WHAT | EXPLOITED | FIXED IN | KEV |
|---|---|---|---|---|
| SA-CORE-2026-017 (18 Nov) | install.php can reinstall a site: takeover or RCE (CVE-2026-132165) | from 19 Nov, 19:00 UTC | 10.6.22 / 11.3.22 / 11.4.13 | 24 Nov · due 27 Nov |
| SA-CORE-2026-019 (25 Nov) | Sites in unusual or incomplete install states stayed open (CVE-2026-136716) | yes, per Drupal | 10.6.23 / 11.3.23 / 11.4.14 + update.php | 27 Nov · due 30 Nov |

Table 6 · Drupal [22, 23], SecurityWeek [24], CISA KEV [1]. End-of-life branches get no fix: upgrade.

### DRUPAL: CHECK FOR TAKEOVER

- Logs: unexpected changes to or by user 1.
- Is user 1's email address one you control?
- Consider resetting user 1's password.
- Secure the installer on every site, patched or not.

Drupal: the vulnerable state is not visible in the interface, and a site already taken over may no longer look vulnerable. [23]

### GEOSERVER · KEV 27 NOV · DUE 30 NOV

| CVE | WHAT (GEOSERVER PROJECT / CISA) |
|---|---|
| CVE-2026-120705 | Unauthenticated WFS GetFeatureById XML injection: read local files or fetch URLs |
| CVE-2026-129243 | Service security rules bypassed with a prefixed service name such as x/WFS |
| chain | CISA: with CVE-2026-129242, -129244 and -129245, unauthenticated RCE |

Fixed in GeoServer 3.0.2, 2.28.6 and 2.27.7, released 19 October; details were published on 23 November. The project page does not mention exploitation; CISA's listing does. [25][1]

1PASSWORD TODOIST POLINRIDER

# One developer account, wide reach

Three stories, one lesson: an account that can change code or pipelines is a production credential.

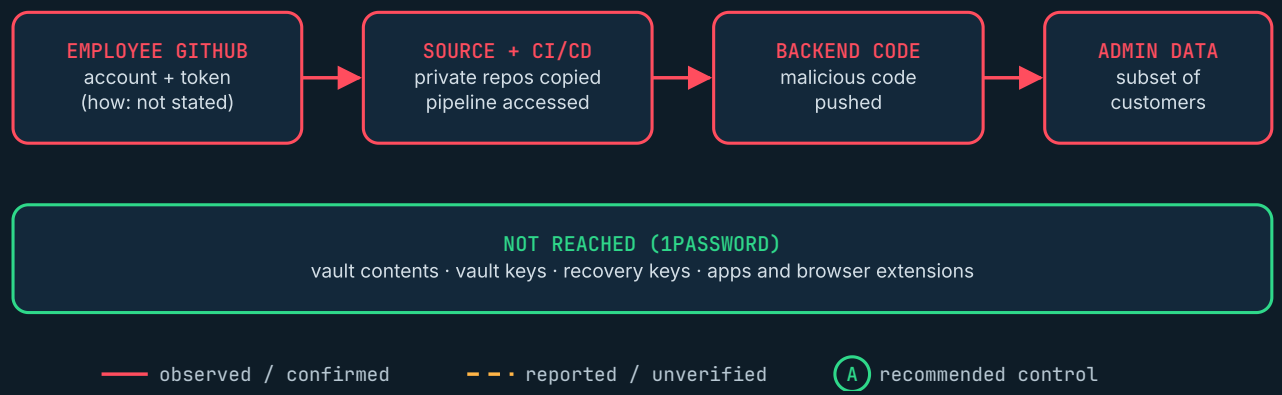



Figure 5 · The 1Password incident as the company describes it [26]. MAG212 CYBER diagram.

## 1PASSWORD · DISCLOSED 25 NOV

With an employee's GitHub account and a stolen token, the attacker copied source code, reached CI/CD and pushed code that downloaded customer administrative data: names, emails, IDs, public keys, SRP parameters and some link tokens. Vaults were not reached; 1Password says no customer action is required. [26][27]

## POLINRIDER · 26 NOV

SafeDep found a Python loader in 375 repos; Apiiro, via The Hacker News, estimates 7,609 across 2,330 accounts. It fetches its next stage from an Ethereum transaction and rewrites the developer's own commits. Researchers link it to North Korea; SafeDep names no group. [29][30]

## TODOIST · 24–26 NOV

| UTC | TODOIST TIMELINE |
|---|---|
| 22 Nov 14:04 | Stolen development credential first used; workflows changed in 3 repos |
| 23 Nov 06:06 | Admin credential for the employee sign-in system taken via automation |
| 09:08 → | Production databases accessed; commands run |
| 12:45–17:12 | Account records exported; tokens, Outlook mail, content searched |
| 17:01–17:42 | Alert on a new admin account; access cut off |

From Todoist's report [28]. About 6% of users had emails and old SHA1 hashes taken; small fractions lost tokens or had content searched for secrets.

### DO THIS WEEK

1. Phishing-resistant MFA and short-lived tokens for every account that can push code or edit workflows.
2. Require review for workflow and build-file changes; branch protection on deployable code.
3. Alert on new admin accounts (how Todoist caught it) and on CI jobs that read secrets they never used before.
4. Search all branches for PolinRider's files (session.py, transport.py in a utils folder; conftest.py calling eth_getTransactionByHash).

CACTI · NO PATCH | NGINX2ROOT | PHPAFTERSHELL | UPLOAD2SHELL

# The servers everyone runs

Four widely run servers had attack research published in the past fortnight. One has no fix at all.

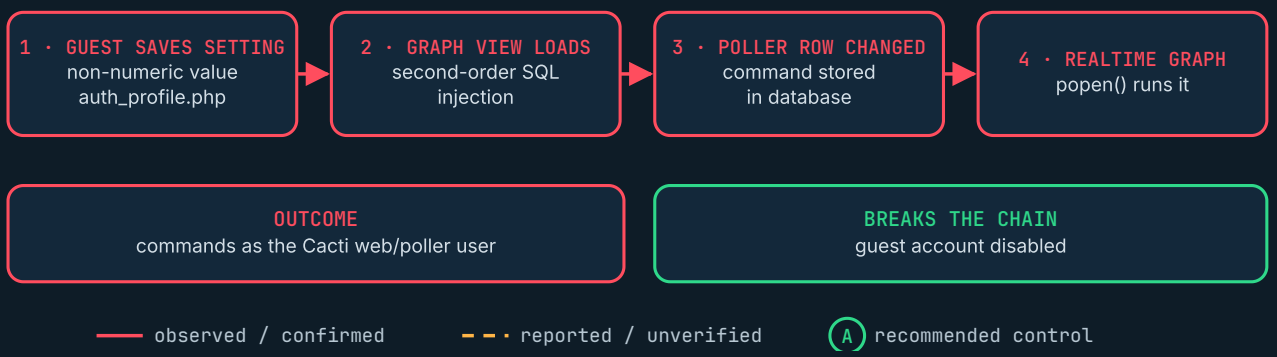



Figure 6 · The Cacti chain as the researcher and watchTowr describe it [34, 35]. MAG212 CYBER diagram.

| BUG | STATUS (28 NOV) | FIX / STOPGAP | KEV |
|---|---|---|---|
| Cacti 1.2.31 "4HTTP2ROOT" (no CVE) | PoC PUBLIC · NO PATCH | Disable guest account; restrict web UI | no |
| NGINX nginx2root (5 CVEs) | NO KNOWN EXPLOITATION | 1.30.7 / 1.31.9; HTTP/2 off blocks only 2 of 5 | no |
| PHP phpAfterShell CVE-2026-126714 | PoC (HARMLESS) · NOT EXPLOITED | 8.2.36 / 8.3.37 / 8.4.28 / 8.5.13 | no |
| Ghostscript Upload2Shell CVE-2026-125396 | PoC · NOT EXPLOITED | 10.08.0 or vendor backport | no |

Table 7 · Sources: watchTowr [34], The Hacker News [35, 33], Censys and nginx.org [31, 32], PHP [36], SecurityWeek [37], pwn.ai [38], AlmaLinux [40], CISA KEV [1].

### CACTI: WHY IT MATTERS

With guest access on, four unauthenticated requests end with commands running as the Cacti web and poller user, not root. Cacti often stores credentials for the network devices it polls, so treat a compromised server as a way into your network. watchTowr lists no CVE, patch or known exploitation. [34]

### NGINX, PHP, GHOSTSCRIPT

- NGINX: Censys counts about 74 million web properties on affected versions; code execution needs an ASLR bypass. [31]
- PHP: an interrupted session write can decode as attacker-chosen objects; turn off session.upload_progress if unused. [36]
- Ghostscript: rated local, yet every path shown was remote (upload, email, print). [38]

# Keys in the cloud, commands in the file share

Two vendor clouds were used against their own customers, and an espionage group hid its orders in public storage.

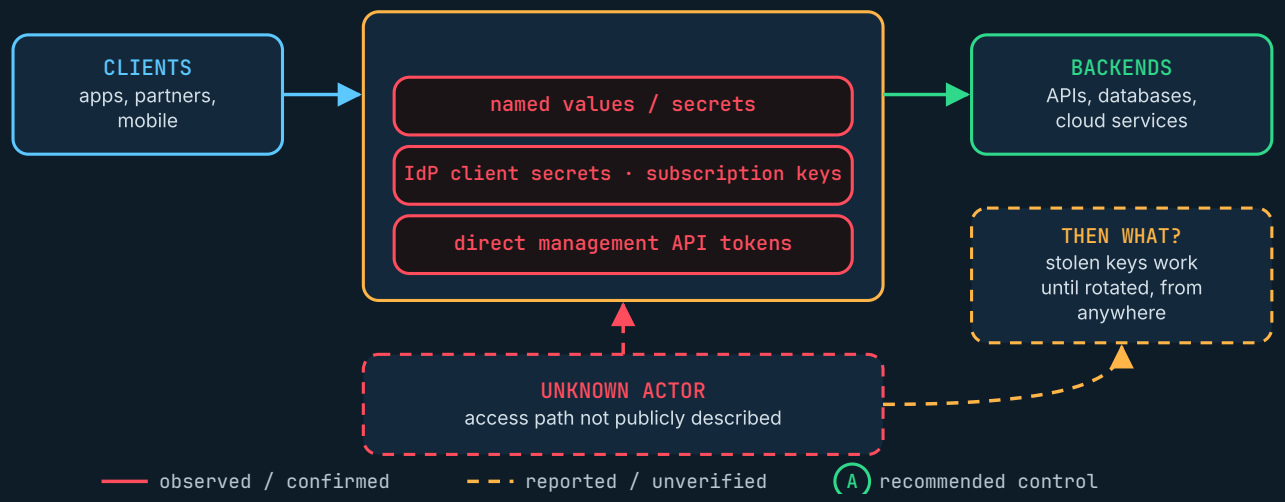



Figure 7 · What sits inside an Azure API Management instance, and why theft matters. The access path is not public, so it is dashed [41, 42]. MAG212 CYBER diagram.

### AZURE API MANAGEMENT · NO CVE

Norway's NSM says an unknown actor went after tokens, secrets and named values in APIM, naming Equinor and Skagerak Energi. Microsoft closed the path on 19 November; only Classic tiers not following its guidance were exposed. Anything taken still works until rotated. [41][42]

Do: rotate named values, IdP secrets, subscription keys and backend credentials.

### GL.iNET GOODCLOUD · CVEs PENDING

A message-authorisation error in the MQTT broker behind GoodCloud let an attacker send management commands to other customers' routers and KVMs; GL.iNet says malware was installed on some. The cloud is fixed; devices need security firmware. [43][44]

Do: update; if in doubt, flash without keeping settings and replace stored VPN and SSH keys.

### VOLANT MANTICORE · IRAN-NEXUS

Check Point Research (high confidence Iran-nexus; medium confidence linked to MuddyWater alumni) says the group poses as job seekers and seminar hosts. Its KuboShell backdoor polls a Pinata/IPFS file every 60 seconds for commands. Targets: Cyprus telecoms and airlines, then Saudi healthcare. [45]

Do: alert on IPFS and Pinata traffic from hosts that never use them.

### EXPOSED AI SERVERS · RAPID7, 18 NOV

In a sample of 20,354 hosts, Rapid7 found 7,675 Ollama servers open without login; 54.8% showed signs that someone else had used them. It is a sample, not an internet-wide count. [46]

Do: bind to localhost or a private network; put an authenticating proxy in front.

**ALSO** N-able Mail Assure (CVE-2026-134624, SSRF) and MONAI Label (CVE-2026-133968) were both KEV-listed on 23 November with a 26 November deadline. [47][11][1]

# Breaches: confirmed vs claimed

Every row is labelled by how well it is sourced. An anonymous-source story is a reason to watch, not to act.

| ORGANISATION | WHAT IS KNOWN | SOURCING |
|---|---|---|
| 1Password | Employee GitHub account; source code and customer admin data; vaults untouched | COMPANY |
| Todoist | Development key to production in a day; ~6% of users' emails and old hashes | COMPANY |
| FIFA | “Limited set” of personal and business information; method and data types unconfirmed | COMPANY + ANON. |
| European Commission | EU Academy users' names and emails; attack involved AI; no attribution | OFFICIAL |
| European Commission | China-backed group suspected; not fully contained (two unnamed sources) | ANONYMOUS |
| CIA (unclassified system) | Open-source intelligence system breached; resolved (one AP source) | ANONYMOUS |
| myColorado | Digital ID app offline after breach found 18 Nov; data types not stated | STATE |
| Peninsula Energy | Lance uranium project: plant and wellfield control systems; operations suspended | COMPANY |
| N-able Mail Assure | Mail Assure cyberattack; SSRF CVE-2026-134624 fixed and KEV-listed | COMPANY |
| Optimizely | Signup-flow flaw let attackers impersonate customer users; KEV-listed | COMPANY |
| Cleverbridge | Card numbers and CVVs stolen, per its notice | COMPANY |

Table 8 · Sources: 1Password [26], Todoist [28], Al Jazeera and ESPN [53, 54], SecurityWeek [48, 50, 52], Euronews [49], The Record [51], N-able [47], Optimizely [56], BleepingComputer [57].

### WHAT WE LEFT OUT, AND WHY

- Ransomware leak-site claims from the week: unverified, and some sites list fabricated victims.
- Breach totals reported only by aggregators or social media, with no organisation statement we could find.
- Claims that a named group or AI tool was behind an incident, where only one secondary source said so.

### IF YOU ARE A CUSTOMER

- 1Password, Todoist, FIFA, EU Academy: expect phishing that uses the breach as a pretext.
- Todoist: replace any secret ever stored in a task or note.
- Colorado residents: carry physical ID; watch for messages about your digital ID.

# What to do, in order

Ranked by exploitation and deadline. Every action links back to the page with its source.

| WHEN | ROLE | ACTION | PAGE |
|---|---|---|---|
| TODAY | Infra | Juniper Conductor 7.0.5 / 7.1.7 / 7.2.3; Xen Orchestra 6.10.1 / 6.9.2; MiCollab KB000129195. Then hunt. | 04, 07, 08 |
| TODAY | Network | Disable Cacti guest access; restrict Cacti to admin networks. | 11 |
| BY MON | Web | Drupal 10.6.23 / 11.3.23 / 11.4.14 and update.php; check user 1. GeoServer 3.0.2 / 2.28.6 / 2.27.7. | 09 |
| BY MON | Identity | MFA or passkeys on every internet-facing login; list accounts whose passwords never expire. | 05, 06 |
| THIS WEEK | Platform | vCenter then ESX per VMSA-2026-0011; NGINX 1.30.7 / 1.31.9; PHP and Ghostscript updates. | 07, 11 |
| THIS WEEK | Security | Check Point managers: CVE-2026-16232 fix, task history, Internal CA, /etc/ld.so.preload. | 07 |
| THIS WEEK | Dev / CI | Short-lived tokens, reviewed workflow changes, alert on new admins; search repos for PolinRider. | 10 |
| THIS WEEK | Cloud | Rotate every Azure APIM Classic secret; update GL.iNet devices; lock down Ollama hosts. | 12 |

### PATCHED IS NOT THE SAME AS CLEAN

MiCollab was attacked before its fix existed. Drupal says a patched site may already have been taken over. CISA's new KEV entries ask agencies for forensic triage, not just updates. After an exploited flaw, check for signs of past access as well as the version number. [20][23][1]

MAG212 analysis.

### HOW TO KNOW YOU ARE DONE

- Every KEV item due this weekend reports a fixed build, or has an exception with exposure removed.
- No management console reachable from the internet.
- No internet-facing login without MFA.
- Developer and CI tokens rotated where they touched a breached vendor.

### A NOTE ON COMMANDS IN THIS ISSUE

Every command shown is read-only, labelled with its operating system and privilege, and was not tested by MAG212. Run it on systems you own, after taking an image where an intrusion is suspected.

# Three tricks from this week

A ten-minute lesson for every employee, built from this week's real incidents.

### 1 · The “legal department” is calling

Callers claiming to be from legal or the help desk steer staff to a lookalike sign-in page, often on a domain like legal-yourcompany.com registered the day before, then ask for a code or a prompt approval. Unit 42 counts more than 70 such domains since October. [55]

- No one from legal, IT or security needs your one-time code.
- Don't approve a sign-in prompt you didn't start.
- Hang up and call back on a number from the directory.

### 2 · After the breach, the follow-up scam

When a company says names and emails were exposed, scammers follow with messages about “your account”, an invitation or a recovery. 1Password warned its customers to expect exactly this, and says it never asks for a password or Secret Key. [26]

- Don't use links in “security notice” emails; open the app yourself.
- No real support team asks for your password or recovery key.
- Unexpected invitation or recovery email? Ask IT first.

### 3 · Your notes app is not a vault

In the Todoist breach the attacker searched customers' tasks and notes for seed phrases, passwords and API keys. Deleting a note does not cancel a copy someone already took. [28]

- Passwords and keys go in the password manager, nowhere else.
- Never paste a secret into a task, ticket, chat or shared doc.
- Already did? Tell IT and change it; deleting is not enough.

#### FOR ADMINISTRATORS

- Move privileged and help-desk accounts to passkeys first.
- Watch for new domains with your brand plus “legal”.
- Run secret scanning on wikis, tickets and chat, not only code.

#### THREE QUESTIONS FOR YOUR NEXT MEETING

1. Could a caller reset an account by phone today?
2. Which supplier's breach would we warn staff about?
3. Where do we really keep shared passwords?

# Sources (1 of 2)


[1] CISA (GitHub mirror) · checked 28 Nov 2026 · Known Exploited Vulnerabilities catalog, version 2026.11.27

[2] CISA · 25 Nov 2026 · CISA adds 10 known exploited vulnerabilities to catalog

[3] CISA · 27 Nov 2026 · CISA adds three known exploited vulnerabilities to catalog (not loadable from our tools)

[4] Security Affairs · 24 Nov 2026 · CISA adds N-able MailAssure and Project MONAI flaws to KEV

[5] Swiss NCSC (BACS) · 24 Nov 2026 · Cyberattacks involving AI agents: first confirmed cases in Switzerland

[6] The Hacker News · 26 Nov 2026 · Switzerland confirms AI-assisted cyberattacks breached critical infrastructure

[7] BleepingComputer · 25 Nov 2026 · Italy and Switzerland warn of autonomous AI-driven cyberattacks

[8] UK NCSC · Nov 2026 · Familiar weaknesses, exploited faster: defending against agentic cyber attacks

[9] AWS Security Blog (CJ Moses) · 20 Nov 2026 · Chinese-nexus actor's Cairn AI agents found a zero-day on their own

[10] Project MONAI · 18 Nov 2026 · GHSA-qc22-rmgc-vg94: MONAI Label path traversal

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

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

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

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

[15] SecurityWeek · 26 Nov 2026 · Critical Juniper Session Smart Conductor flaw exploited in attacks

[16] eSecurity Planet · 26 Nov 2026 · Juniper Session Smart Conductor RCE exploited: CISA sets Nov. 28 deadline

[17] Juniper Networks · 28 Oct 2026, updated 24 Nov · 2026-10 On-Demand Security Bulletin: Session Smart Router and Conductor (not loadable)

[18] The Hacker News · Nov 2026 · Hackers exploit critical Xen Orchestra flaw (VSA-2026-062)

[19] Mitel · 16 Nov 2026, updated 24 Nov · MISA-2026-0012: MiCollab multiple vulnerabilities (rev 2.0)

[20] Accenture APEX Labs · Nov 2026 · MiCollab exploitation: zero-days used before Mitel's advisory

[21] SecurityWeek · 26 Nov 2026 · Mitel MiCollab zero-days exploited in suspected AI-assisted attacks

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

[23] Drupal Security Team · 25 Nov 2026 · SA-CORE-2026-019: Drupal core access bypass (highly critical)

[24] SecurityWeek · 26 Nov 2026 · Drupal installer patch left a gap attackers are already exploiting

[25] GeoServer project · 23 Nov 2026 · GeoServer security update (CVE update)

[26] 1Password · 25 Nov 2026 · Update on November 2026 security incident

[27] The Hacker News · 26 Nov 2026 · 1Password hacked, customer data and source code stolen in GitHub account breach

[28] Todoist · 24 Nov 2026, updated 26 Nov · Security incident in November 2026

[29] SafeDep · Nov 2026 · PolinRider Python loader reads payloads from Ethereum calldata

[30] The Hacker News · 26 Nov 2026 · North Korea-linked PolinRider poisons over 7,600 GitHub repositories

[31] Censys · 18 Nov 2026, updated · nginx2root advisory

[32] nginx.org · Nov 2026 · nginx security advisories

[33] The Hacker News · 26 Nov 2026 · ThreatsDay: 10M NGINX services at risk, 250+ malicious extensions

[34] watchTowr · 26 Nov 2026 · 4HTTP2ROOT: Cacti zero-day FAQ

# Sources (2 of 2)


[35] The Hacker News · 27 Nov 2026 · Unpatched Cacti zero-day enables RCE in just four HTTP requests via guest access

[36] PHP (php-src) · 19 Nov 2026 · GHSA-fm2m-fjf5-v3cp: partially overwritten session files can lead to RCE

[37] SecurityWeek · 23 Nov 2026 · phpAfterShell vulnerability revives PHP2Shell's attack path

[38] pwn.ai (Paulos Yibelo) · 21 Nov 2026 · How we hacked the pipes: Upload2Shell (CVE-2026-125396)

[39] The Hacker News · 22 Nov 2026 · Researchers demonstrate Ghostscript sandbox-escape RCE via crafted files

[40] AlmaLinux · 22 Nov 2026, updated 23 Nov · Upload2Shell (CVE-2026-125396) fixes

[41] Norwegian National Security Authority (NSM) · 20 Nov 2026, updated 23 Nov · NSM deler tiltak mot sårbarhet i Azure API Management

[42] SecurityWeek · 23 Nov 2026 · Azure flaw exploited to target secrets at Norwegian energy firms

[43] GL.iNet · 20 Nov 2026, updated 22–23 Nov · Security notice: GoodCloud remote management incident

[44] SecurityWeek · 23 Nov 2026 · GL.iNet routers, KVMs compromised via remote management service flaw

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

[46] Rapid7 · 18 Nov 2026 · Open by default. Already occupied: exposed self-hosted AI servers

[47] N-able · 22 Nov 2026 · CVE-2026-134624: Mail Assure LDAP sync connection check SSRF

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

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

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

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

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

[53] Al Jazeera · 26 Nov 2026 · FIFA says personal and business information stolen in cyberattack

[54] ESPN · 26 Nov 2026 · FIFA hit by cyberattack as hackers gain access to personal and business data

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

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

[57] BleepingComputer · 22 Nov 2026 · Cleverbridge warns hackers stole credit card numbers, CVVs in data breach


## HOW WE VERIFIED THIS ISSUE

- KEV dates and descriptions come from CISA's catalog data (official GitHub mirror, version 2026.11.27, released 27 Nov 18:03 UTC). CISA's 27 November alert page did not load for us.
- Primary sources read this week include the Swiss NCSC, Broadcom, Mitel, Accenture, Drupal, GeoServer, GreyNoise, Amazon, 1Password, Todoist, GL.iNet, NSM, PHP, watchTowr, Censys and Rapid7.
- Juniper's bulletin did not load: its details come from SecurityWeek, eSecurity Planet and CISA. FIFA's method and the Commission and CIA attributions come from anonymous sources and are labelled.
- Items published before 22 November are dated. Every command shown is read-only and was not 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 · 28 November 2026
Understand the threat. Build the defense.