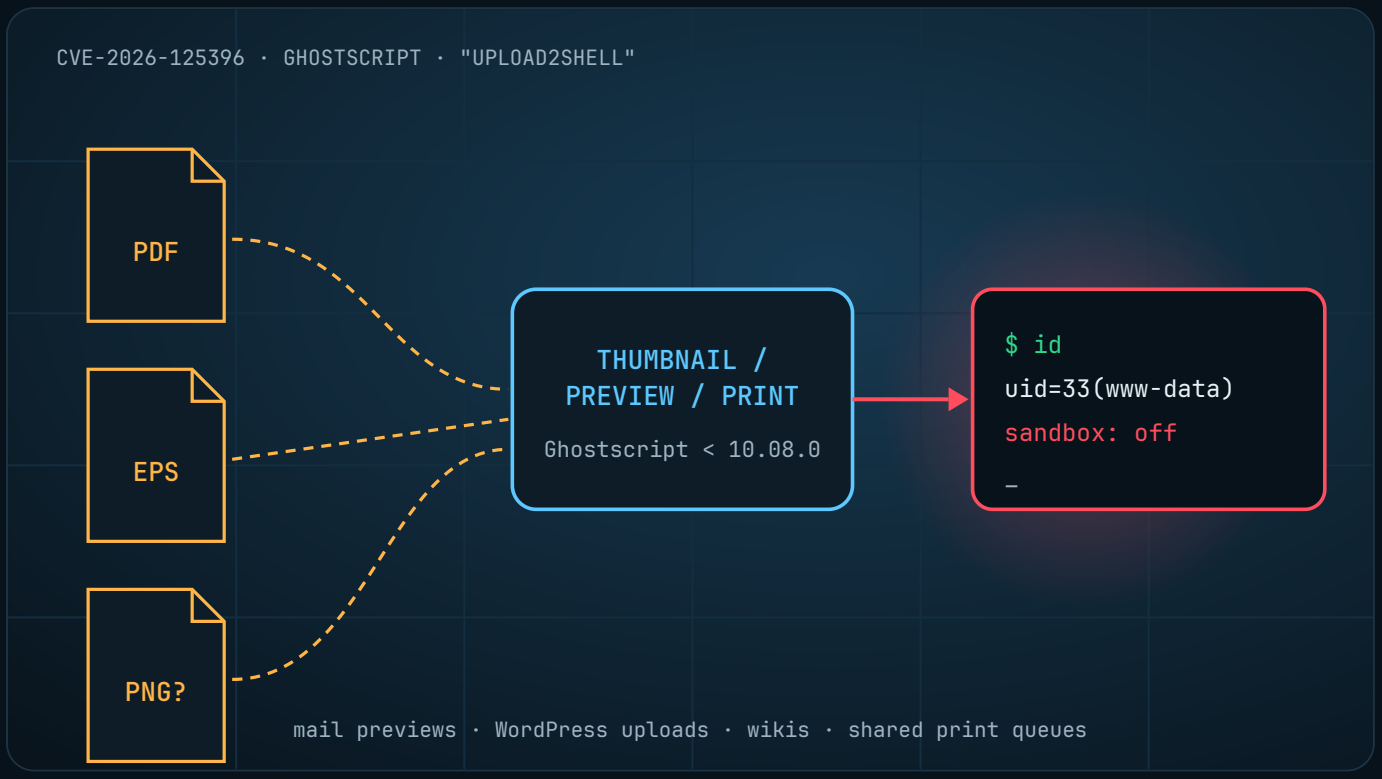
MAG212
CYBER

DAILY

Monday, 23 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 7:00 AM PT



GHOSTSCRIPT · CVE-2026-125396

One upload, one shell

Researchers turned a Ghostscript bug into command execution through ordinary file uploads, mail previews and print jobs. The fix shipped in September; some enterprise distributions were still unpatched in mid-November. Also: AI hosts admit prompt leaks, and a China-aligned group spies through a rebuilt VPN.

03 Upload2Shell: how one file becomes a shell
04 Who is exposed, and how to fix it
05 AI providers now admit prompt leaks
06 Webworm turns a VPN into a spy bridge
07 Patch board: Tomcat, Puppet, PAN-OS, N-able
08 Public sector: FBI, USDA, Vermont, Charleston
09 Identity and payments: Entra, Cleverbridge

10.08.0
Ghostscript fixed release

4
AI providers disclose leaks

TODAY
4 KEV fixes due · 4 more Tue

1 DEC
Puppet KEV deadline

What matters today

Developments published or updated 21–23 November. Monday brings a KEV deadline and a file-upload lesson.

Files are code

A Ghostscript use-after-free lets a crafted PDF or image switch off the sandbox. pwn.ai reached shells through mail previews, WordPress uploads and a shared print queue. [1][2]

AI hosts confirm the leaks

Phala, Together, Novita and Atlas Cloud have now published notices on prompt exposure; Together says an AI coding agent leaked the key. [8][9][10][11]

Spying with legitimate tools

Rapid7 says the China-aligned Webworm group rebuilt SoftEther VPN Bridge to tunnel into European government networks, with no malware to detect. [13]

Public sector, still unexplained

No official word on the FBI NCIC intrusion. USDA calls its incident a cyberthreat; Vermont and Charleston County deal with their own. [21][23] [27][28]

THE THREE PRIORITY ACTIONS

1. **Close today's KEV list: vCenter, Expressway, Roller, SAP NetWeaver.**
   Federal deadline is today, 23 November; Outlook, Chromium, BroadWorks and Openwave follow tomorrow. [5]
2. **Update every Ghostscript your apps load to 10.08.0 or a vendor backport.**
   Check containers and appliances too; Debian 12, Amazon Linux and SUSE were still open on 12 November. [1]
3. **Rotate any secret ever pasted into a prompt sent via a router or reseller.**
   Phala, Atlas and Novita all tell users to treat secrets sent to affected models as exposed. [8][10][11]

STATUS AT A GLANCE

ISSUE	STATUS	FIX / NEXT STEP
Ghostscript CVE-2026-125396	PUBLIC POC · NOT IN KEV	10.08.0 / backport
Tomcat CVE-2026-133325	FIX NOT YET RELEASED	TLS 1.2 for cluster
Puppet CVE-2026-115731	EXPLOITED	KEV due 1 Dec
KEV batch of 20 Nov	EXPLOITED	due today

CONTENTS

03 Upload2Shell attack chain
04 Upload2Shell: fix and verify
05 AI provider disclosures
06 Webworm SoftEther bridge
07 Patch board
08 Public-sector incidents
09 Entra Connect Health; Cleverbridge
10 Briefs
11 Defender's Action Desk
12 Awareness: downloads and callers
13 Sources

GHOSTSCRIPT · CVE-2026-125396 · UPLOAD2SHELL

One upload, one shell: how a Ghostscript bug reached WordPress, webmail and print servers

Ghostscript quietly renders PDFs and PostScript behind thumbnails, previews and print queues. Researchers showed a crafted file can switch off its sandbox and run commands.

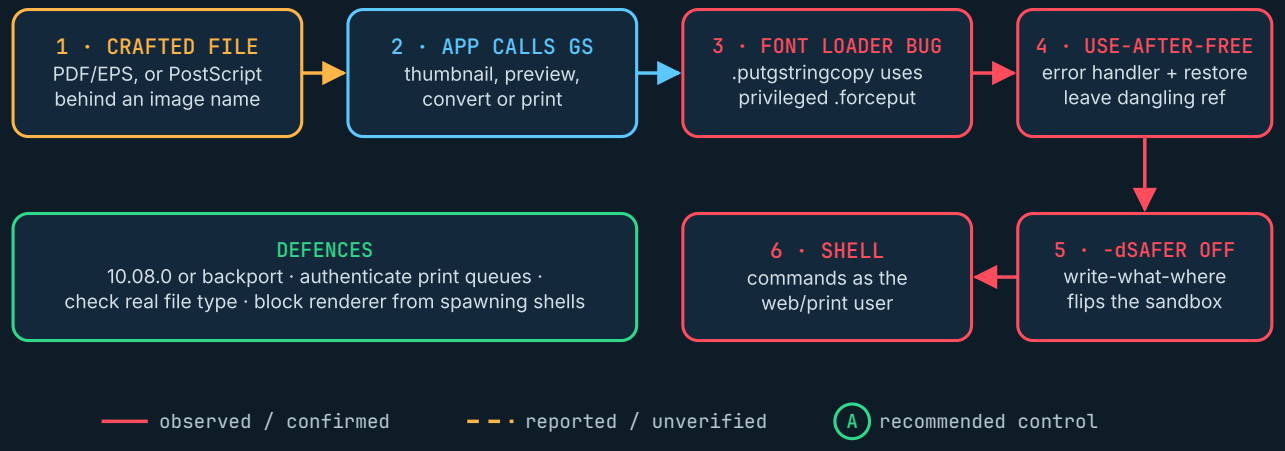


Figure 1 · The Upload2Shell chain as described by pwn.ai [1]. Steps 1–6 were demonstrated by the researchers; no in-the-wild exploitation is reported. MAG212 CYBER diagram.

WHAT HAPPENED

On 21 November Paulos Yibelo of pwn.ai published "Upload2Shell", CVE-2026-125396. A helper in Ghostscript's Type 1 font loader calls a privileged operator; a document's own error handler can catch a failure there, leaving a reference that a later `restore` frees. The researchers turned that use-after-free into a write that switches off `-dSAFER`. [1][2]

Artifex fixed it in Ghostscript 10.08.0 on 8 September. A developer called the code path "an ancient piece of code well known to be a vulnerability". [1][2]

SEVERITY: READ IT CAREFULLY

Rated CVSS 4.0 8.5 with a *local* attack vector, yet every path the researchers showed was remote: an upload, an email, a print job. Scanners that rank by vector may under-rate it. [1][2]

EXPLOITATION

- Public proof of concept only writes renderer memory; it does not run commands.
- No in-the-wild use reported; not in CISA KEV.

DON'T MIX UP

CVE-2026-39919 is a different Ghostscript bug (heap overflow, October), also fixed in 10.08.0. [4]

Who is exposed, and how to close it

The library is patched. The work is finding every copy your applications actually load, including the ones inside containers and appliances.

APPLICATIONS WITH A DEMONSTRATED PATH [1] · GOOGLE CLOSED ITS PATH 10 NOV [3]

WHERE	PATH SHOWN BY PWN.AI
Webmail	Roundcube 1.7.2: preview built when the message is viewed; Plesk Obsidian 18.0.79
Printing	Debian 13 CUPS through an unauthenticated shared IPP queue
WordPress	Core via CVE-2026-65640 (fixed 7.0.4); Forminator and Essential Addons upload forms
Docs and wikis	MediaWiki PdfHandler, DokuWiki, Mayan EDMS, Paperless-ngx, ResourceSpace
Libraries	Pillow EPS, PHP Imagick, libvips, Matplotlib, ComfyUI, Home Assistant and more

DISTRIBUTION PATCH STATUS · PWN.AI SNAPSHOT 11–12 NOV

DISTRIBUTION	STATUS
Debian 13 · Ubuntu	FIXED DSA-6516-1 · USN-8949-1
Arch, Alpine, Fedora Rawhide, Homebrew	FIXED 10.08.0
Debian 12	VULNERABLE
Amazon Linux 2 / 2023	FIX PENDING
SLES 12–16 · openSUSE Leap 16	IN PROGRESS
RHEL, Rocky, Alma, Oracle	NOT CHECKED

Snapshot, not today's state. Backports keep old version numbers: check the changelog [3].

Linux · bash | user | READ-ONLY | NOT TESTED BY MAG212

check ghostscript

```
gs --version
dpkg -l ghostscript              # Debian/Ubuntu
rpm -q ghostscript               # RHEL/SUSE/Amazon
docker run --rm IMAGE gs --version  # IMAGE = your image
```

10.08.0 or later, or a vendor build listing CVE-2026-125396, is fixed. Generic commands; not tested by MAG212.

REMEDIATE · CONTAIN · VERIFY

1. Update Ghostscript everywhere it is loaded (containers, bundles, appliances) and restart; authenticate shared print queues.
2. Check real file types before previews; confine the renderer so it cannot start a shell. Do not rely on -dSAFER alone.
3. Verify: re-run version checks; look for shells spawned by gs on web, mail and print hosts since September (MAG212 suggestion).

DRAGOS CANARIES · PROVIDER DISCLOSURES

The AI hosts start to explain how prompts leaked

Four inference providers have now published their own accounts. One root cause stands out: an AI coding agent that pushed a key to a public repository.

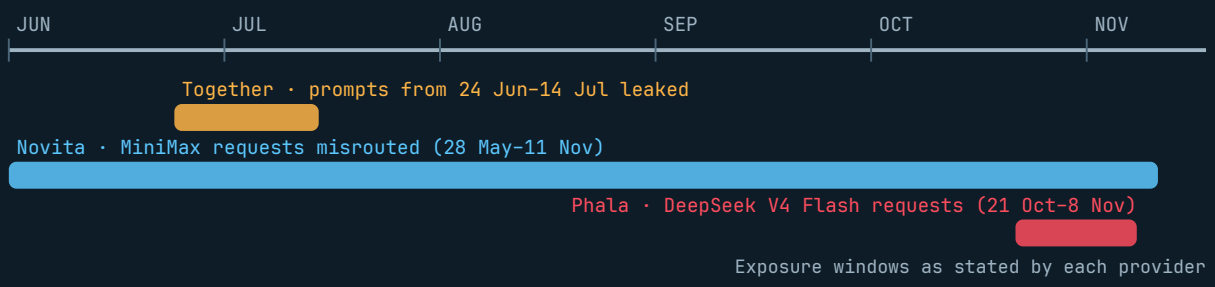


Figure 2 · Exposure windows in each provider's own notice [8, 9, 10]. Novita's window began 28 May. MAG212 CYBER diagram.

WHAT EACH PROVIDER SAYS

PROVIDER	WHAT IT DISCLOSED	ADVICE TO USERS
Phala (10 Nov)	Two intrusions by one actor via a legacy internet-facing service and loopback-trusting admin interfaces; a new GPU server ran production traffic without full hardening	Rotate all secrets in prompts sent 21 Oct–8 Nov
Together AI (21 Nov)	An AI coding agent committed a credential to a public repo; it opened a private store of prompt samples that an unauthorised party downloaded	Enable ZDR; new accounts now default to it
Novita (22 Nov)	Routing misconfiguration sent some MiniMax requests to MiniMax's official API, 28 May–11 Nov; test URLs were opened, AWS test keys were not used	Rotate secrets sent; models suspended
Atlas Cloud (23 Nov)	Links in prompts sent via MiniMax's API were opened by a third party; it stopped using that API and left OpenRouter	Treat secrets sent to those models as exposed

WHAT IS STILL NOT CONFIRMED

- Which three providers OpenRouter removed; it still has not named them [7, 12].
- Whether these four are the three breaches Dragos found [6].
- Whether the unnamed Chinese AI lab in Dragos's research is MiniMax.

WHAT TO DO

- Rotate any key, token or password ever sent in a prompt through a router or reseller.
- Pin your upstream provider; a privacy flag binds only the first hop [6].
- Stop AI coding agents from committing secrets: pre-commit scanning, no long-lived keys in their reach.

RAPID7 · WEBWORM · SOFTETHER

A VPN that isn't malware, used for spying on governments

Rapid7 found a China-aligned group bridging European government networks to its own servers with a rebuilt, legitimate VPN tool. Antivirus has nothing to flag.

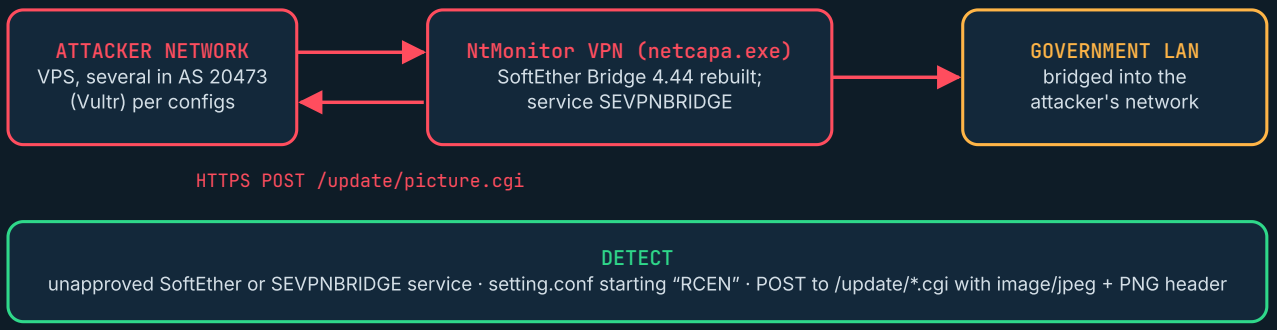


Figure 3 · How the NtMonitor bridge works, per Rapid7 [13]. Indicators may change; Rapid7 expects the actor to rotate endpoints. MAG212 CYBER diagram.

WHAT HAPPENED

On 19 November Rapid7's Milan Spinka described "NtMonitor VPN": SoftEther VPN Bridge 4.44 build 9807, "not trojanized, but rebuilt from source". It runs as `netcapa.exe` under the stock service name `SEVPNBRIDGE`, with an encrypted `setting.conf` and renamed web endpoints so normal clients cannot connect. Rapid7 attributes it to Webworm with moderate confidence; targets are government bodies, mainly in Europe. [13]

WHY IT WORKS

Every file is a legitimate open-source build, so hash and antivirus checks see nothing. The bridge places the attacker on the government network as if it were local. Detection has to rely on what should not be there.

Windows · PowerShell | admin

READ-ONLY | NOT TESTED BY MAG212

hunt for the bridge

```
Get-Service SEVPNBRIDGE -ErrorAction
SilentlyContinue
Get-CimInstance Win32_Service |
  Where-Object { $_.PathName -match
'netcapa' }
```

Any result on a host with no approved SoftEther use needs investigation. Generic queries built from Rapid7's indicators; not tested by MAG212.

IF YOU FIND IT

1. Isolate the host; capture memory and the config file.
2. Use Rapid7's GitHub IOCs and YARA rule to scope other hosts.
3. Hunt for how the actor got admin rights; reset those credentials.

Patch board: what to fix this week

Two exploited flaws without a fix path you control, one critical flaw without a release yet, and eight federal deadlines in two days.

NEW OR UPDATED, 19–23 NOVEMBER

PRODUCT · CVE	ISSUE	STATUS	ACTION
Apache Tomcat · CVE-2026-133325	Cluster using TLS 1.3 + TLS-PSK lets an unauthenticated node join	CRITICAL · NO EXPLOIT	11.0.30 not yet released: use TLS 1.2 for cluster traffic
Puppet Server · CVE-2026-115731	Crafted report from any CA-signed agent runs code; weak autosign makes it unauthenticated	EXPLOITED · KEV	PE 2023.8.13 / 2025.12.1 / 2026.0.1; Core 8.22.2 / 9.1.3; restart. Due 1 Dec
PAN-OS / Panorama · CVE-2026-123633	nginx HTTP/2 flaws reach devices with HTTP/2 enabled	CVSS 9.2 · NO EXPLOIT	12.1.7-h15, 11.2.10-h19, 11.2.13-h6; or disable HTTP/2
N-able Mail Assure · CVE-2026-134624	SSRF in LDAP sync connection check, CVSS 9.3	FIXED IN CLOUD	Build 20261121.1943; link to the breach not stated
Idunno.AntiCsrf · CVE-2026-131914	Deserialization in an abandoned ASP.NET module (2008)	EXPLOITED · NO PATCH	Find and remove the module; no maintainer

Sources: Apache [14, 15], KEV and Help Net Security [5, 16], Palo Alto [17], N-able [18, 19], Mandiant [20]. Tomcat 10.1.63 and 9.0.125 are reported by the press but not checked on Apache's pages.

KEV DEADLINES: TODAY AND TOMORROW

CVE	PRODUCT	DUE
CVE-2026-123890	VMware vCenter	TODAY
CVE-2026-76466	Cisco Expressway	TODAY
CVE-2026-129448	Apache Roller	TODAY
CVE-2025-42884	SAP NetWeaver Portal	TODAY
CVE-2026-124194	Microsoft Outlook	24 Nov
CVE-2026-125350	Chromium	24 Nov
CVE-2026-20320	Cisco BroadWorks	24 Nov
CVE-2026-111793	Openwave Webtop	24 Nov

No new KEV entries 21–23 November as of 06:00 PT [5].

PUPPET: WHAT TO CHECK

- Unknown or recently signed agent certificates.
- Autosign rules that sign anything.
- Port 8140 reachable from untrusted networks.

TOMCAT: IS IT YOU?

Only clusters using Apache Tribes with TLS-PSK over TLS 1.3, and only if the cluster port is reachable. Most Tomcat servers do not cluster. Our reading of Apache's advisory.

Four public-sector incidents, no official link between them

Officials said before the FBI news that recent outages were upgrades, not attacks. Nobody has revisited that since. Here is what each case confirms.

WHERE EACH CASE STANDS, 23 NOVEMBER

INCIDENT	WHAT IS CONFIRMED	WHAT IS NOT
FBI NCIC	FBI investigating (anonymous sources: CNN 2, NBC 2, AP 1, ABC 1). DNI Clayton: origin and scope will be shared later	Any official statement; scope; entry; data; actor
USDA (FPAC)	Security incident found by USDA's operations centre; all database passwords reset, taking farm-loan and payment apps offline. An undersecretary called it a "cyberthreat"	Attacker; entry; the claim that no data was lost is early
Vermont Valcour	State police dispatch and records system taken offline after a vendor flagged a potential threat; 911 unaffected	Cause; data
Charleston County, SC	Attack identified 16 Nov; county confirms data was copied; state police investigating	Count; actor

Sources: ABC [21], KCRA [22], AP [34], Nextgov [23], GovTech [24], ABC News 4 [25], Valley News [27], Holy City Sinner [28]. No FBI, DOJ, CISA or CJIS statement on NCIC by our cutoff.

THE USDA LESSON: RESETS CAN BE OUTAGES

USDA's response, resetting every database password in every environment, is what took farmer payment tools down for days. Resets are right after a compromise, but plan them: map which services use each credential, stage the rotation, and tell users it is security work. USDA's public site said "maintenance" while staff were told "security incident". [23][24]

FOR STATE AND LOCAL IT

- Contract for vendor breach notice on dispatch and records systems: Vermont learned from its vendor.
- Keep a manual fallback for dispatch and records.
- Keep public and staff messages consistent.
- For NCIC users: the CJIS checks in our 22 November issue still apply.

DID OFFICIALS LINK THE OUTAGES?

On 18 November, before the NCIC reports, DNI Clayton said there was "no indication that these events are related" and DHS leadership said adversaries were not behind recent outages. USDA's undersecretary has since called its incident a cyberthreat, not an update. [26][25]

Microsoft tells some tenants their admin contacts were read; Cleverbridge confirms card theft

Two breaches that hand attackers exactly what they need for the next phishing email.



Figure 4 · Entra Connect Health timeline from Microsoft's customer notice as reported [30]. MAG212 CYBER diagram.

ENTRA CONNECT HEALTH

A Microsoft notice, seen via a sysadmin forum and reported on 22 November, says attackers read tenant metadata through a cloud-side flaw in Entra Connect Health. Microsoft says passwords, hashes, tokens and keys were not exposed, and no customer patch is needed. No tenant count, actor or CVE has been given. [30]

FOR ENTRA ADMINS

- Check Azure Service Health for the advisory.
- Expect targeted phishing aimed at named admins.
- Enforce phishing-resistant MFA and PIM for admin roles.
- Review sign-in and audit logs since July.

CLEVERBRIDGE

The payment platform used by many software sellers detected unauthorised activity on 4 November and began notifying people on 20 November. It says this was not ransomware. Reporting says card numbers, expiry dates and security codes were copied; Cleverbridge's own update does not list those fields. No count or entry method has been given. [29]

FOR CUSTOMERS AND MERCHANTS

- If you bought software through a Cleverbridge checkout, watch card statements and replace the card if notified.
- Merchants: expect customer questions; prepare a support script.
- Treat calls or emails “about the breach” with suspicion.

Also this weekend

DETECTION

VirusTotal now tags files that really encrypt

A new `encrypts-files` sandbox tag is applied only when user files are verified as encrypted during execution. Since 17 November it matched 55 of 328,257 new files with no benign hits reported. One Python locker it caught scored 0 on antivirus engines. [31]

MALWARE CAMPAIGN

Fake GTA 6 PC launchers on 355 domains

VECERT's "CyberLeek" report lists over 355 domains and subdomains pushing a fake Windows launcher for GTA 6, a game with no PC release. No malware family or hashes were published; 355 counts infrastructure, not victims. [32]

RANSOMWARE CLAIM

Nvidia: Gentlemen deadline is Saturday

No proof posted and no new Nvidia statement. Nvidia said it found no sign its systems were affected and is looking at a possible third-party partner incident. The gang's countdown ends 28 November. [33]

AI · MEDICAL SOFTWARE

MONAI Label: still no patched release

The advisory behind Amazon's Cairn AI-agent case still lists no CVE and no fixed version. Turn on authentication, keep it off untrusted networks, run it unprivileged. Covered in our 21 and 22 November issues.

A TECHNIQUE TO BRIEF YOUR HELP DESK ON

Email bombing followed by a fake "IT support" call on Microsoft Teams keeps resurfacing: thousands of sign-up emails flood an inbox, then a caller offers to fix it and asks for remote access. Fortra describes campaigns of about 10,000 messages sent through bulk-mail services. This is a recurring pattern, not a new incident this weekend. [35]

NOT INCLUDED, AND WHY

- Bell Canada breach reports: could not verify against a primary source by our cutoff.
- Leak-site claims since Friday: not re-checked for this issue.
- OpenRouter's customer email about MiniMax: seen only in secondary reports; the providers' own notices are on page 5.

Your work list for the week

Ordered by urgency. Each row points to the page with evidence and verification steps.

WHEN	TEAM	ACTION	SEE
TODAY	Vuln mgmt	Close KEV items due 23 Nov: vCenter, Expressway, Roller, SAP NetWeaver Portal.	p.07
TUESDAY	Endpoint	Close KEV items due 24 Nov: Outlook, Chromium, BroadWorks, Openwave.	p.07
48 H	Linux / web / mail	Ghostscript to 10.08.0 or vendor backport on every host, container and appliance; restart.	p.04
48 H	Print	Require authentication on shared print queues; take IPP sharing off untrusted networks.	p.04
48 H	Dev / AI	Rotate secrets ever sent via AI routers or resellers; block agents from committing keys.	p.05
THIS WEEK	Windows / SOC	Hunt for SEVPNBRIDGE / netcapa.exe and unapproved VPN bridges.	p.06
BY 1 DEC	Config mgmt	Patch Puppet Server; review signed agent certificates and autosign.	p.07
THIS WEEK	Identity	Entra: check Service Health; enforce phishing-resistant MFA for admins.	p.09
THIS WEEK	Web apps	Find and remove Idunno.AntiCsrf; it is exploited and unmaintained.	p.07

ONE-PAGE HUNT SHEET

`Ghostscript`	Child processes such as `sh` or `bash` spawned by `gs` on web, mail and print hosts since September.
`SoftEther`	Service `SEVPNBRIDGE`, `netcapa.exe`, a `setting.conf` starting “RCEN”, POSTs to `/update/picture.cgi`.
`Puppet`	Newly signed agent certificates; reports from unknown agents.
`AI keys`	Cloud API calls from keys that only ever appeared in prompts.
`Entra`	Phishing aimed at the admin contacts listed in your tenant.

BEFORE YOU CLOSE A TICKET

- No KEV CVE from the two batches open in the scanner.
- gs --version passes on every host and image.
- No unapproved VPN bridge services anywhere.
- Every rotated key has a new owner and expiry.

COMMAND SAFETY

Every command in this issue is read-only. They are generic tools built from vendor or researcher indicators, not taken from vendor advisories. None was run by MAG212 for this issue; try them on one system first.

Free downloads and helpful callers

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



Two tricks, one rule: you start the contact, not them.

Get software from the official store. Call the help desk on the number you already have.

This week: fake GTA 6 launchers on 355 domains · email bombing before fake support calls

Figure 5 · Two social-engineering paths from this week's reports [32, 35]. Conceptual illustration, MAG212 CYBER.

FOR EVERY EMPLOYEE

- There is no PC version of GTA 6. A site offering one is lying about everything else too.
- Never run a .exe from a ZIP you downloaded from an ad or search result.
- A sudden flood of emails is a warning sign; report it and wait.
- If “IT” calls first, hang up and call the help desk number you already know.

FOR ADMINISTRATORS

- Block executables in ZIPs from newly registered domains at the proxy.
- Restrict external Teams chats and calls to approved domains.
- Make remote-support tools require a help-desk ticket number.
- Treat uploaded files as code: patch Ghostscript and sandbox previews.

FOR BUSINESS LEADERS

- Ask how your staff can verify the IT team in under a minute.
- Make reporting a suspicious call praised, not embarrassing.
- Check that your help desk will never ask for remote access unprompted, and say so to staff.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Where do our people get software, and what stops them installing from anywhere else?
2. How does an employee know a caller is really from IT?
3. Which of our systems turn uploaded files into previews, and who patches them?

Sources

[1] pwn.ai (Paulos Yibelo) · 21 Nov 2026 · How We Hacked the Pipes: Upload2Shell (CVE-2026-125396)

[2] The Hacker News · 22 Nov 2026 · Researchers demonstrate Ghostscript sandbox-escape RCE via crafted file uploads

[3] iTnews · 23 Nov 2026 · AI-found Ghostscript flaw turned file uploads into remote code execution

[4] BleepingComputer · Oct 2026 · Ghostscript flaw lets hackers hijack servers via PDF uploads (CVE-2026-39919, a different bug)

[5] CISA · checked 23 Nov 2026 · Known Exploited Vulnerabilities catalog (JSON)

[6] Dragos (HD Moore) · 19 Nov 2026 · Three breaches, endless leaks: Your AI supply chain needs canaries

[7] OpenRouter · 22 Nov 2026 · Data Processing Incidents on Inference Providers

[8] Phala · 10 Nov 2026 · November preliminary incident report

[9] Together AI · 21 Nov 2026 · Security event: prompt leakage for requests in June and July of 2026

[10] Novita · 22 Nov 2026 · MiniMax requests privacy notice

[11] Atlas Cloud · 23 Nov 2026 · Our security and privacy commitment

[12] SecurityWeek · 23 Nov 2026 · AI inference providers failed to detect hacking and prompt theft, says Dragos

[13] Rapid7 (Milan Spinka) · 19 Nov 2026 · Spying on governments, no malware: Webworm's custom toolkit and SoftEther bridge

[14] Apache Tomcat · 19 Nov 2026 · Fixed in Apache Tomcat 11.x security vulnerabilities (CVE-2026-133325)

[15] Cybersecuritynews · 20 Nov 2026 · Critical Apache Tomcat flaw lets remote attackers join trusted server clusters

[16] Help Net Security · 19 Nov 2026 · Puppet fixes exploited report-processing flaw and certificate bypass

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

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

[19] The Hacker News · 22 Nov 2026 · N-able discloses critical Mail Assure flaw

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

[21] ABC News · 21 Nov 2026 · FBI's national crime database targeted in hack

[22] KCRA (Hearst) · 22 Nov 2026 · FBI investigating suspected hack of national crime database, AP reports

[23] Nextgov/FCW · 19 Nov 2026 · USDA grapples with security breach as IT staff take multiple systems offline

[24] GovTech · Nov 2026 · Department of Agriculture suffers outage after reported cyber incident

[25] ABC News 4 (TNND) · Nov 2026 · Hackers allegedly breach USDA system used to pay farmers

[26] KCRA (Hearst) · 18 Nov 2026 · Mullin doesn't suspect cyberattacks are behind recent tech outages

[27] Valley News · 19 Nov 2026 · Vermont takes Valcour police records system offline after potential security threat

[28] Holy City Sinner · Nov 2026 · Charleston County shares update on cyberattack

[29] Cybersecuritynews · 23 Nov 2026 · Cleverbridge data breach

[30] Cybersecuritynews · 22 Nov 2026 · Microsoft Entra Connect Health flaw exposed tenant data

[31] VirusTotal (Karl Hiramoto) · 20 Nov 2026 · Catching ransomware: introducing the encrypts-files tag

[32] VECERT Foundation · 20 Nov 2026 · CyberLeek malware campaign: 355 domains, fake GTA 6 PC launchers

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

[34] AP via PBS NewsHour · 21 Nov 2026 · AP source: FBI investigating apparent hack of its key national criminal justice database

[35] Fortra · undated · Mail bombing as pretext for Teams vishing attack (background)

HOW WE VERIFIED THIS ISSUE

- Primary sources read: pwn.ai's Upload2Shell write-up, Apache's Tomcat advisory page, the CISA KEV JSON, Rapid7's Webworm report, Palo Alto's and N-able's advisories, Mandiant's disclosure, and the Phala, Together, Novita and Atlas Cloud notices.
- NCIC still rests on anonymous sources; the Entra Connect Health notice was seen via press and a sysadmin forum, not a Microsoft page; Cleverbridge's card-data fields come from press reporting.
- Not reachable: Artifex advisory page, Red Hat CVE pages, Rapid7's GitHub IOC list. Leak-site claims were not re-checked. The National Cyber Director appointment is left out by editorial choice.
- 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 · 23 November 2026
Understand the threat. Build the defense.