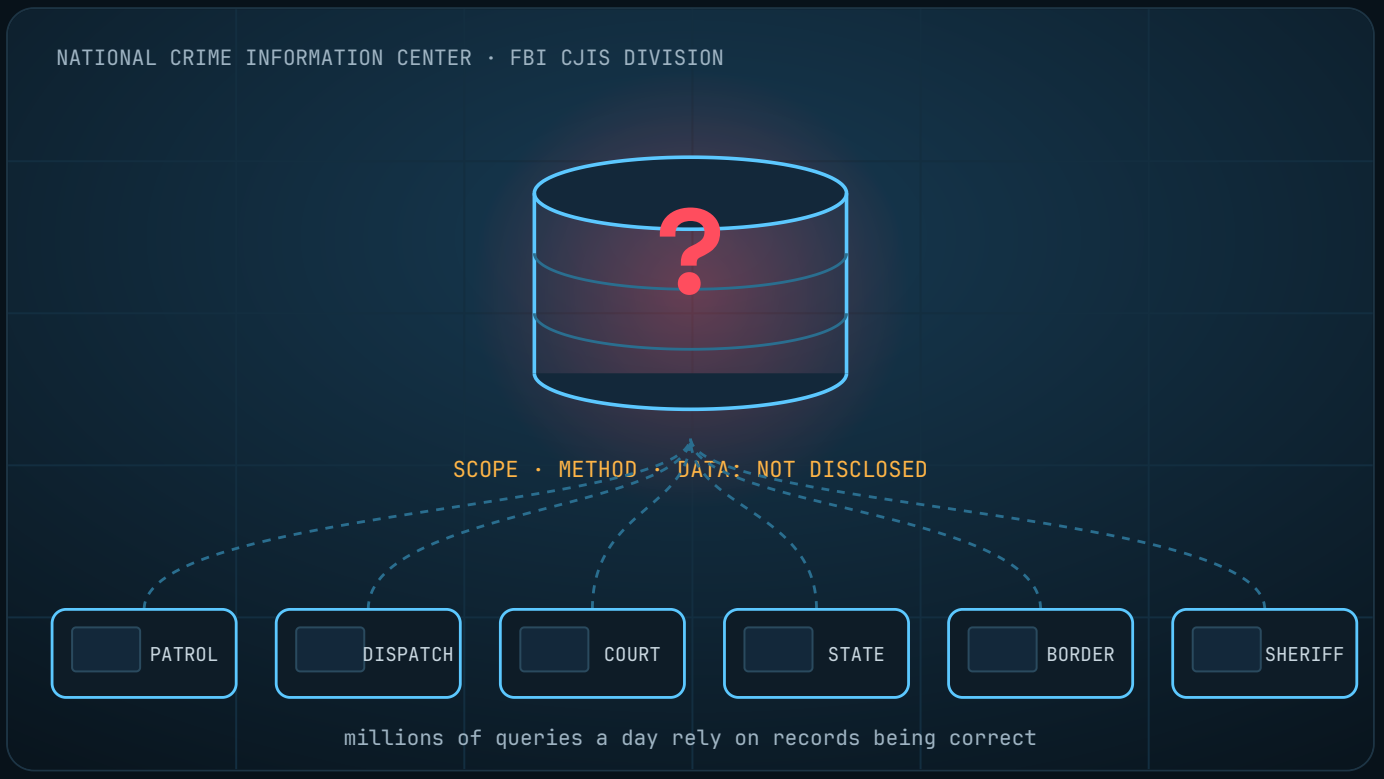
MAG212
CYBER

DAILY

Sunday, 22 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 7:00 AM PT



FBI · NATIONAL CRIME INFORMATION CENTER

Can police trust the record?

The FBI is investigating an apparent hack of NCIC, the database police across the US query millions of times a day. The FBI has not confirmed it, and nothing is known yet about scope or method. Also today: a GPGME flaw reaches mail clients and Flatpak, and an AI agent is hijacked by one web page.

03 FBI crime database: what is known
04 For police IT: what to do now
05 GPGME: one bad key, many apps
06 Meta Muse: an AI agent hijacked
07 Signal vs. AI assistants; WhatsApp fix
08 Monday deadline: 8 exploited flaws
09 The supplier breach ledger

UNCONFIRMED
NCIC hack: FBI declines comment

2.3.1
GPGME fix · legacy 1.24.4

8
KEV fixes due 23–24 Nov

2.26.35.74
WhatsApp Android minimum

What matters today

Developments published or updated 20–22 November: a quiet weekend for new flaws, a busy Monday for deadlines.

A national police system in question

CNN and AP report, citing unnamed sources, that the FBI is investigating an apparent hack of NCIC. The FBI declined to comment. Scope, method and data are unknown. [1][3][4]

One crafted key, many applications

GnuPG fixed a double free in GPGME that a very long OpenPGP user ID can trigger. Mail clients, XMPP clients, Samba and Flatpak embed the library. No attacks reported. [8][11]

AI agents as the new endpoint

NebuSec chained a stale browser and a kernel bug to take over a Meta Muse agent's cloud VM from one web page. Signal is blocking OS AI assistants from reading chats. [13][17]

Deadlines and the supply chain

Eight KEV fixes fall due on 23–24 November. Vendor breaches keep surfacing: Wellington IT, TfL, Rakuten, N-able, and the JPMorgan, Visa and Mastercard suppliers. [21][25][28]

THE THREE PRIORITY ACTIONS

1. **Close Monday's KEV list: vCenter, Expressway, Roller, SAP.**
   Federal deadline 23 November; Outlook, Chromium, BroadWorks and Openwave follow on 24 November. Neither Broadcom nor Cisco yet acknowledges exploitation in its advisory. [21][22][23]
2. **Update GPGME everywhere it lives: 2.3.1, 1.24.4 or Gpg4win 5.1.2.**
   Patch the distro package, then rebuild anything that links GPGME statically. [8][11]
3. **Agencies on CJIS: verify MFA, audit logs and record validation now.**
   Do not wait for FBI detail. Confirm who can query, review unusual access, and confirm NCIC hits before acting, as the rules already require. [5][7]

STATUS AT A GLANCE

ISSUE	STATUS	FIX / NEXT STEP
FBI NCIC intrusion	UNDER INVESTIGATION	no detail released
GPGME CVE-2026-129975	PATCHED · NO ATTACKS	2.3.1 / 1.24.4
WhatsApp CVE-2026-23871	SUSPECTED ABUSE	Android 2.26.35.74+
KEV batch of 20 Nov	EXPLOITED	due 23 Nov

CONTENTS

03 FBI NCIC: what is known
04 Police IT: CJIS checks
05 GPGME CVE-2026-129975
06 Meta Muse hijack
07 Signal and WhatsApp
08 KEV deadlines
09 Supplier breach ledger
10 Briefs
11 Defender's Action Desk
12 Awareness: breach-notice scams
13 Sources

FBI · NCIC · UNCONFIRMED BY THE FBI

The FBI investigates an apparent hack of its national crime database

Two outlets report, from unnamed sources, that the National Crime Information Center was targeted. The FBI has said nothing. Here is what is known, what is not, and why the database matters.

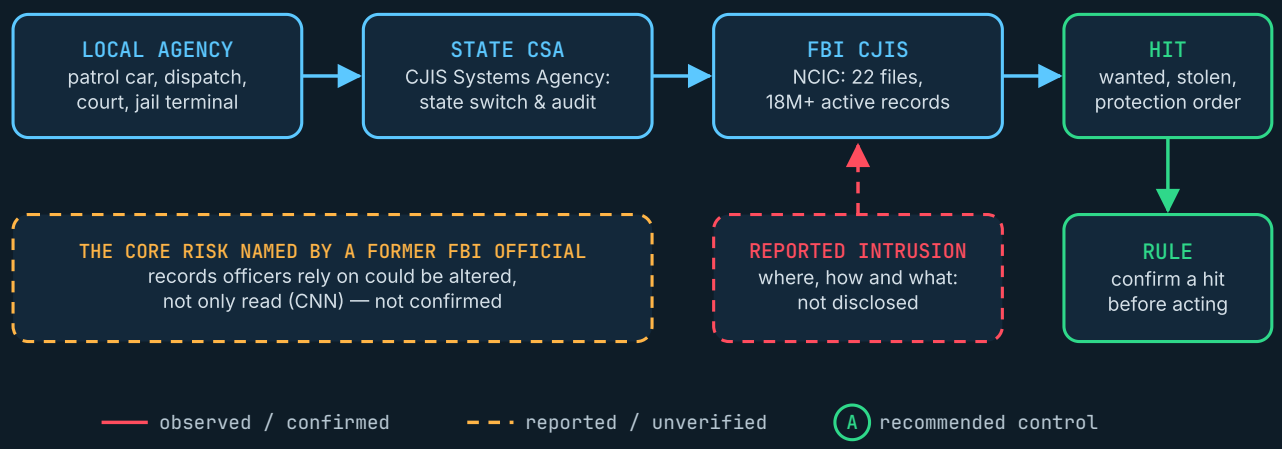


Figure 1 · How an NCIC query travels. System flow per FBI documentation [6]; record counts are FBI figures cited by Forbes [5]; the intrusion box is deliberately empty because no source says where it happened. MAG212 CYBER diagram.

WHAT HAPPENED

On the night of Friday 20 November, CNN reported that the FBI is investigating a hack targeting NCIC, citing two people briefed on the investigation. On Saturday the Associated Press confirmed the investigation through one person familiar with the matter, who was not authorised to discuss it. [3][1]

The FBI declined to comment to AP and did not respond to CNN or BleepingComputer. BleepingComputer says the activity was discovered "in recent days". No advisory from the FBI or CISA had appeared by our cutoff. [1][4]

WHY IT MATTERS

NCIC holds files on wanted people, stolen property, protection orders and more: by FBI figures cited by Forbes, 22 files and more than 18 million active records, queried millions of times a day. [5][6]

CONFIRMED

- The FBI is investigating (per AP's and CNN's sources).
- The FBI has not commented.

REPORTED, NOT CONFIRMED

- That NCIC itself was the target.
- That records could be altered, not just read (a concern raised by a former official).

UNKNOWN

- Entry point, timing and attacker.
- Whether data was read, taken or changed.
- Any effect on state and local agencies.
- Any link to the FBI's earlier 2026 incidents: none shown.

For police and public-sector IT: what to do before the FBI says more

You cannot patch what has not been disclosed. You can make sure your own access to criminal justice information is tight, logged and checked.

TIMELINE OF REPORTING

WHEN	WHAT	SOURCE
Fri 20 Nov, night	CNN reports the FBI is investigating a hack targeting its crime database (two sources)	[3]
Sat 21 Nov	AP confirms through one person familiar with the matter; FBI declines comment	[1]
Sat 21 Nov	SecurityWeek, BleepingComputer and Forbes follow; no new official detail	[2, 4, 5]
Sun 22 Nov, 7 AM PT	No FBI, DOJ or CISA statement found at our cutoff	—

CJIS SECURITY POLICY: CONTROLS TO RE-CHECK

CJIS CONTROL (v6.1)	WHAT TO CHECK THIS WEEK
Multi-factor authentication	Every account that reaches CJI, privileged or not, local or remote
Compromised-password list	Updated at least quarterly; passwords screened against it
Vulnerability scanning	At least monthly, and after any incident involving CJI
Encryption	256-bit for CJI in transit and at rest
Record ownership	Your agency validates its own NCIC entries on schedule
Hit confirmation	Confirm with the originating agency before acting on a hit

As summarised by BleepingComputer's v6.1 explainer [7] and NCIC rules cited by Forbes [5]. Priority 1 controls enforceable since 1 Oct 2024. Audit against the policy text on le.fbi.gov.

INVESTIGATE: SUGGESTED CHECKS

1. Ask your state CSA for your agency's query logs; look for off-shift, bulk or unfamiliar-terminal queries.
2. List every account with CJI access; remove leavers and shared logins; confirm MFA.
3. Review recent entries, modifications and clears on records your agency owns.

IF YOU FIND SOMETHING

1. Preserve logs, then report through your CSA and FBI CJIS channels.
2. Disable affected accounts; rotate credentials and certificates.
3. Re-validate your records before officers rely on them.

MAG212 ANALYSIS

The worst case is tampering, not theft: a cleared warrant, a removed protection order, a stolen car that no longer shows. NCIC's own rule, confirming a hit with the originating agency before acting, deserves strict enforcement until the FBI explains what happened. This is our assessment, not a reported fact.

GNUPG · GPGME · CVE-2026-129975

One crafted key, many applications

A double free in GPGME, the library mail clients, XMPP clients, Samba and Flatpak use to talk to GnuPG, is triggered by importing a key with an oversized user ID.

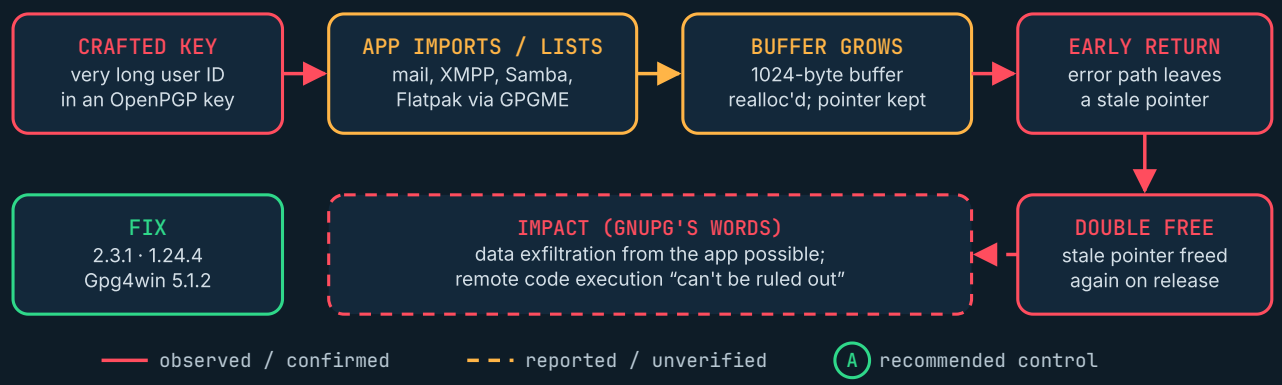


Figure 2 · The bug path described in GnuPG's advisory and tracker task T8557 [8, 9]. Impact wording is GnuPG's own. MAG212 CYBER diagram.

WHAT HAPPENED

Published 20 November: two readers in `src/engine-gpg.c`, `read_status()` and `read_colon_line()`, grow a buffer but store the new pointer only at the end; an early error return frees it twice. Disclosure moved up from 25 November because GitLab had to update early for Ruby2Shell. [8][9]

WHO IS AFFECTED

All GPGME versions before 2.3.1 (and before 1.24.4 on the legacy branch), whether linked as a shared library, a Windows DLL or statically. C++/Qt bindings need no change. No CVSS, no exploitation reported. [8][10][12]

Linux · bash | user | READ-ONLY

NOT TESTED BY MAG212

check installed GPGME

```
dpkg -l 'libgpgme*'      # Debian / Ubuntu
rpm -q gpgme             # RHEL / Fedora / SUSE
pkg-config --modversion gpgme   # build hosts
```

Compare the version with the table below. Generic package queries, not from GnuPG's advisory. Static builds will not show up here: check each vendor.

FIX STATUS · GNUPG [8, 10] · DEBIAN [11] · OTHER DISTROS NOT REACHABLE

PRODUCT	FIXED VERSION	STATUS
GPGME · legacy branch · Gpg4win	2.3.1 · 1.24.4 · 5.1.2	FIXED
Debian 12 · Debian 13	1.18.0-3+deb12u1 · 1.24.2-3+deb13u1	FIXED
Debian forky (testing)	–	VULNERABLE
Ubuntu, RHEL, SUSE	check vendor tracker	NOT VERIFIED

REMEDIATE · VERIFY

1. Update the package and restart services that load GPGME (mail, XMPP, Samba); Gpg4win 5.1.2 on Windows. Rebuild static builds and Flatpak runtimes.
2. Verify with the version checks; ask vendors of appliances and mail clients for fixed builds.

META MUSE · NEBUSEC RESEARCH · FIXED

One web page, one hijacked AI agent

Researchers took over a Meta Muse agent's cloud machine after a user asked it to save a malicious page. The lesson for every company deploying agents: they inherit the bugs of the browser and kernel they run on.

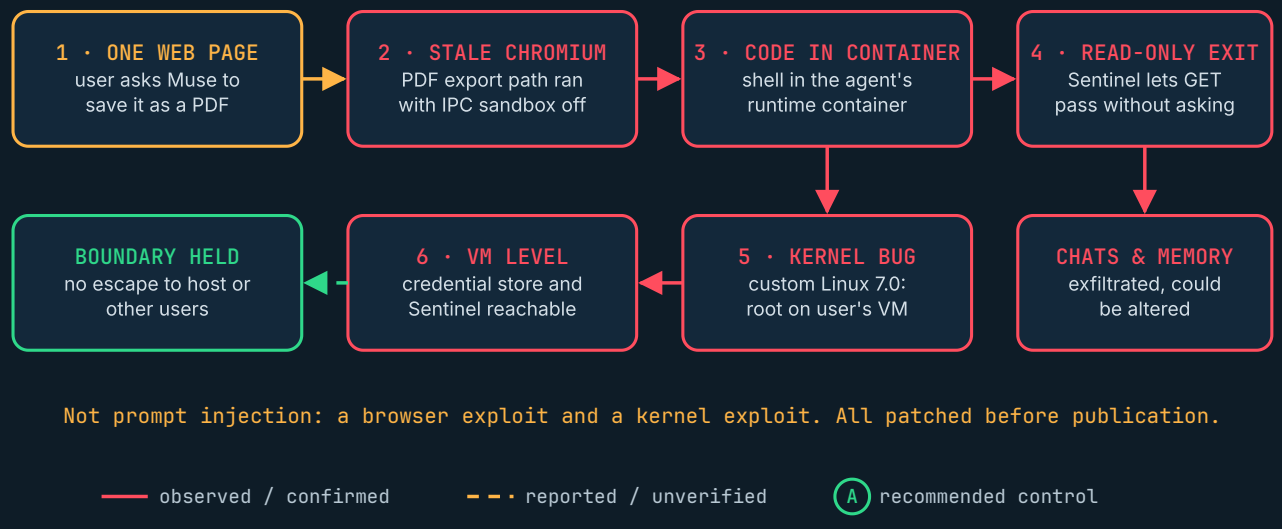


Figure 3 · The exploit chain as published by NebuSec on 20 November [13, 14]. Observed in NebuSec's research environment; no attacks on real users reported. MAG212 CYBER diagram.

WHAT HAPPENED

Each Muse user gets a small cloud VM; the agent runs in a container inside it, and a guard called Sentinel controls outbound traffic. Muse's bundled Chromium lagged behind upstream, and its PDF export ran without the IPC sandbox. A crafted page gave NebuSec shell access, which it calls a "0.5-click" attack. [13]

Under the default setting Sentinel asks before writes but lets read requests (GET, HEAD, OPTIONS) through, so conversation history and memories left without a prompt. A kernel exploit then gave root on the VM. NebuSec does not say connector credentials were actually taken. [13][14]

STATUS

NebuSec says the Muse team knew of every finding and had patched all exploits before publication. No report or fix dates were given, Meta has not commented publicly, and no in-the-wild use is reported. Do not confuse this with Meta's separate $1.2M Muse bug-bounty disclosure earlier in November. [13][15]

FOR TEAMS RUNNING AI AGENTS

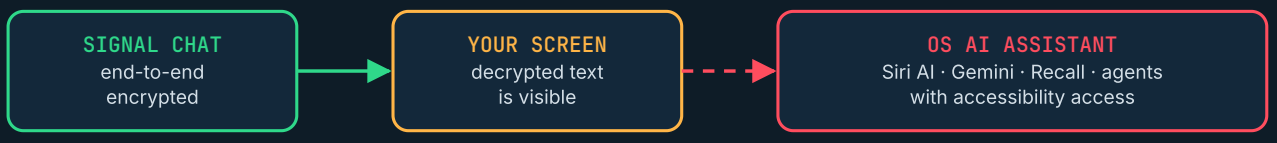
- Patch the agent's browser and kernel on the browser's schedule, not the product's.
- Egress filters must inspect GET query strings: "read-only" is not "no data out".
- Keep one tenant per VM; it is what stopped this chain spreading.
- Log what the agent fetched and exported, and alert on spikes.

STILL UNKNOWN

- When NebuSec reported the bugs and when each was fixed.
- Which kernel CVEs applied: NebuSec names none.
- Whether any real user's data was touched before the fixes.

Signal shuts the screen to AI assistants; WhatsApp fixes a scam helper

The weak point is now the device, not the encryption.



Encryption protects the message in transit, not the pixels on the display.

Figure 4 · The endpoint problem Signal describes in its 20 November post [17]. Conceptual diagram, MAG212 CYBER.

On 20 November Signal president Meredith Whittaker said operating-system AI agents are an “existential threat” to Signal's mission. Signal now blocks or limits screen capture where it can, but calls the remedy incomplete: files on the device, notifications and agents using accessibility permissions (a “skeleton key”) are not covered. [17][18]

SIGNAL'S PROTECTION BY PLATFORM [17] · THN SAYS iOS DEFAULT IS ON [18]

PLATFORM	WHAT SIGNAL DOES	GAP
iOS 27	“Block Siri AI” setting stops screenshots inside the app	default state not stated by Signal
Android	Detects an AI assistant reading the screen, turns on Screen security	some vendor builds not covered
Windows 11	Screenshot blocking on by default since 2025 (against Recall)	—
macOS	Cannot block Siri AI today	add Signal to Siri › Excluded Apps

WhatsApp's November advisory fixes three bugs. Its team found CVE-2026-23871 while disrupting a scam campaign; SecurityWeek calls it low impact. [19][20]

WHATSAPP NOVEMBER ADVISORY [19] · NO CVSS GIVEN

CVE	WHAT	FIXED IN	EXPLOITED?
CVE-2026-23871	Crafted Click-to-WhatsApp ad reply leaks the phone's IP address	Android 2.26.17.4	SUSPECTED, IN SCAMS
CVE-2026-102769	SQL injection from an unofficial client's “order details” message	Android 2.26.35.74	NO
CVE-2026-44908	Certificate-chain check for Meta AI's confidential backend	iOS 2.26.24.72 · Android 2.26.23.74	NO

WHAT TO DO

- Update WhatsApp on Android to 2.26.35.74+; keep Signal's screen protections on. Mac: System Settings › Siri › Excluded Apps › add Signal (Signal's path; may vary).
- MDM teams: treat OS AI assistants with screen or accessibility access as a data-loss path, and set policy for them.

CISA KEV · BOD 26-04

Monday's list: eight exploited flaws due in two days

No new entries over the weekend: the moment to close the ones already listed, several at the network edge.

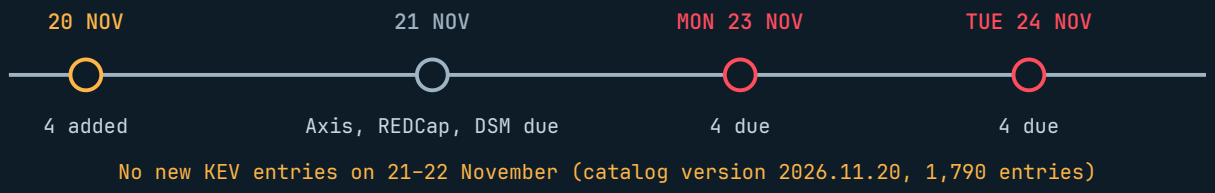


Figure 5 · KEV deadlines from the CISA catalog JSON, version 2026.11.20 [21]. MAG212 CYBER diagram.

DUE 23–24 NOVEMBER

CVE	PRODUCT · FLAW	DUE	VENDOR ADVISORY SAYS
CVE-2026-123890	VMware vCenter · auth bypass (VMDIR)	23 Nov	no exploitation noted (VMSA .1)
CVE-2026-76466	Cisco Expressway · hard-coded credentials	23 Nov	"not aware of malicious use" (v1.0)
CVE-2026-129448	Apache Roller · XML-RPC deserialization	23 Nov	KEV: same bug as CVE-2026-82384
CVE-2025-42884	SAP NetWeaver Portal · JNDI injection	23 Nov	—
CVE-2026-124194	Microsoft Outlook	24 Nov	—
CVE-2026-125350	Chromium	24 Nov	—
CVE-2026-20320	Cisco BroadWorks · XXE	24 Nov	—
CVE-2026-111793	Openwave Webtop Media Transcoder	24 Nov	—

KEV catalog [21]; vendor wording from Broadcom [22] and Cisco [23] as of 22 Nov.

WHY VENDOR PAGES ARE NOT ENOUGH Broadcom's VMSA-2026-0009.1 and Cisco's advisory (still v1.0) do not acknowledge exploitation, although CISA lists both. Prioritising by vendor wording alone under-rates them. [21] [22][23]

Linux/macOS · bash, curl, jq | user | READ-ONLY | NOT TESTED BY MAG212

kev due dates

```
KEV=https://raw.githubusercontent.com/cisagov/kev-
data/develop/known_exploited_vulnerabilities.json
curl -s "$KEV" | jq -r '.vulnerabilities[] | select(.dueDate=="2026-11-23" or
.dueDate=="2026-11-24") | [.cveID,.product] | @tsv'
```

Lists the CVEs due on those two dates; compare with your scanner's findings.

The breach ledger

Most of this week's breach news has one shape: the company you deal with was not the one breached. Here is where each case stands as of 22 November.

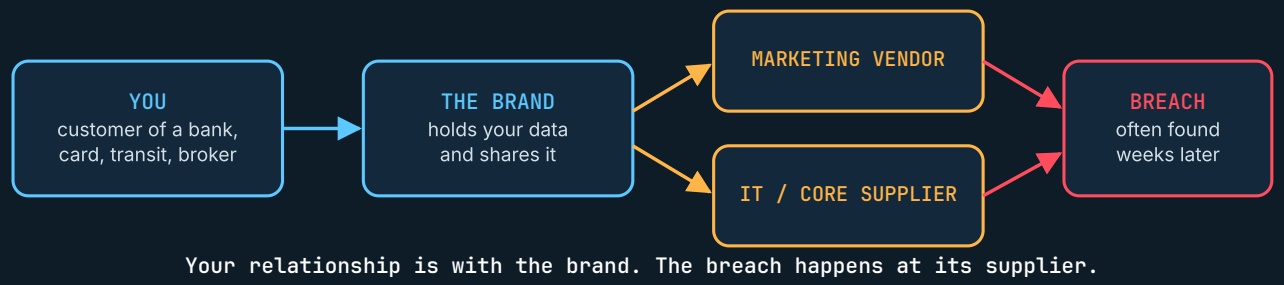


Figure 6 · Third-party data flow. Conceptual diagram, MAG212 CYBER.

WHERE EACH CASE STANDS

VICTIM / SUPPLIER	CONFIRMED	CLAIMED OR UNVERIFIED	SEE
JPMorgan, Visa, Mastercard · unnamed vendors	Vendor incidents; contact data such as names and emails; payment systems unaffected	n0n gang's role; Reuters' review of 16,000+ JPMorgan emails	[25, 26]
Wellington IT · ~40–43 Irish credit unions	Exploited 2–4 Oct, closed 6 Oct; payee names, IBANs, sort codes, addresses	total members affected	[28, 29]
Transport for London · its own mail systems (not a supplier)	~265,000 photocard holders: names, addresses, dates of birth, security Q&A	—	[30, 31]
Rakuten Securities	Up to 11.25M accounts (IDs); up to 4.47M with richer personal and financial data	—	[32]
N-able · Mail Assure / SpamExperts	Server breached; stored credentials “may” have been accessed; tokens revoked	—	[27]
The Container Store	Systems restored; financial data “does not appear” taken	n0n's earlier listing unaddressed	[33]

Updates since our 20 November issue are limited: no vendor has been named in the payment-card cases and no new counts have been confirmed.

FOR MSPs USING N-ABLE MAIL ASSURE

N-able rotated internal credentials, revoked customer API and OAuth tokens and reset local-user passwords. Expect integrations to break; re-issue tokens from the portal once it is back, and check for logins you do not recognise. [27]

FOR CREDIT UNION AND BANK CUSTOMERS

Wellington IT's exposed data includes saved payees and IBANs: ideal material for fake “your payee details changed” messages. Confirm any change by calling a number you already trust. Ireland's minister of state called the six-week notification gap “not acceptable”. [28]

Also this weekend

STATE GOVERNMENT

West Virginia Legislature knocked offline

An incident that began on 19 November took the Legislature's website and some IT systems down. Outside specialists were brought in; it appears limited to the Legislature. Officials would not say whether it was ransomware, and no group has claimed it. [35]

FEDERAL · OUTAGE

NSA network back after three-day disruption

The NSA says its internal classified network is back to normal after a disruption it blames on PHP maintenance and patching. Officials deny a cyberattack; The Record notes it could not independently confirm that. [36]

RANSOMWARE CLAIM

Nvidia: Gentlemen deadline is 28 November

The gang has shown no proof. Nvidia says it found no indication its own systems were affected and is looking at a possible incident at a third-party partner. Watch for a leak or a quiet deadline next Saturday. [34]

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 (≤ 0.8.5 affected; fix in PR #1915). Enable `MONAI_LABEL_AUTH_ENABLE=True`, keep it off untrusted networks and run it unprivileged. [24]

LEAK-SITE CLAIMS, 20–22 NOV · NOT CONFIRMED BY VICTIMS

NAMED ORGANISATION	SECTOR	GROUP CLAIMING
Regions Behavioral Hospital (US)	Healthcare	INC Ransom
Fort Smith EMS (US)	Healthcare	The Gentlemen
Dallas Fort Worth Fertility Associates (US)	Healthcare	“Barracuda”
Lucid Motors	Automotive (possible re-listing)	Inception
Invicta Watch Group	Retail	Qilin
Kang Chiao International School (Taiwan)	Education	Osiris

Source: ransomware.live tracker [38]. A listing is a claim, not proof of a breach. Sovcali claimed Lucid in August 2026.

ALSO NOTED

ITEM	WHY IT MATTERS	SEE
Ukraine and FBI arrest four in ransomware ring	Police say $40.5M+ taken from at least 28 firms using fake IT-support calls with AI voice messages	[37]
n0n extortion group (background)	SOCRadar: gets in with stolen or weak credentials, not exploits; sometimes destroys data	[39]
Roller KEV entry	CISA: same bug as CVE-2026-82384 but a wider range of versions; recheck what you patched	[21]

Your work list for the week ahead

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

WHEN	TEAM	ACTION	SEE
MONDAY	Vuln mgmt	Close KEV items due 23 Nov: vCenter, Expressway, Roller, SAP NetWeaver Portal.	p.08
TUESDAY	Endpoint	Close KEV items due 24 Nov: Outlook, Chromium, BroadWorks, Openwave.	p.08
48 H	Linux / mail	Update GPGME (2.3.1 / 1.24.4 / Gpg4win 5.1.2); restart mail, XMPP, Samba; rebuild static apps.	p.05
48 H	Police IT	Confirm MFA on all CJI accounts; pull NCIC query logs from your CSA; review record changes.	p.04
48 H	MSP	N-able Mail Assure: re-issue API and OAuth tokens; review logins.	p.09
THIS WEEK	Mobile / MDM	WhatsApp Android to 2.26.35.74+; set policy for OS AI assistants with screen access.	p.07
THIS WEEK	AI platform	Patch agent browsers and kernels; inspect GET query strings at egress.	p.06
THIS WEEK	Finance / AP	Verify any “payee details changed” request by phone (Wellington IT data).	p.09
THIS WEEK	Awareness	Warn staff about breach-notice phishing tied to bank, card and transit breaches.	p.12

ONE-PAGE HUNT SHEET

GPGME	`dpkg -l` / `rpm -q` versions below the fixed builds; static binaries from vendors.
CJIS	Queries outside shift patterns, bulk queries, new terminals or vendor accounts.
KEV	Scanner findings for the 8 CVEs; vCenter TCP 2012 reachable from user networks.
AI agents	Unusual volumes of agent page fetches or exports; GET requests with long query strings.
Mail	Messages referencing a real breach and asking to “verify” or “activate monitoring”.

BEFORE YOU CLOSE A TICKET

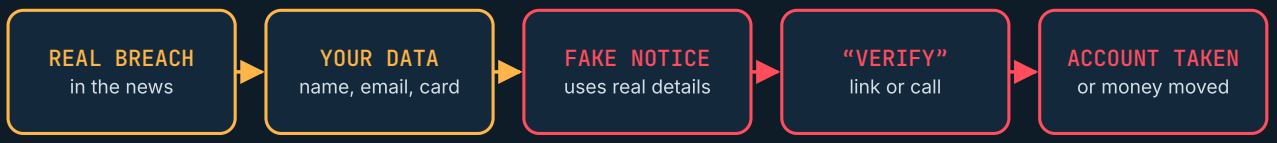
- Scanner shows none of the 8 KEV CVEs open.
- GPGME version check passes on every host and image.
- Every CJI account has MFA and a named owner.
- MSP integrations work with freshly issued tokens.

COMMAND SAFETY

Every command in this issue is read-only. The package queries and the jq filter are generic tools, not taken from vendor advisories; menu paths come from Signal's and WhatsApp's own guidance and may differ by version. None was run by MAG212 for this issue; try them on one system first.

When the breach email is the attack

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



A real breach makes a fake message believable.

Go to the company yourself: its app, its website typed by hand, or the number on your card.

This week: bank and card vendors · Irish credit unions · TfL Oyster photocards · Rakuten Securities

Figure 7 · How breach-notice scams work. Conceptual illustration, MAG212 CYBER [25, 28, 30].

FOR EVERY EMPLOYEE

- A message that mentions a real breach, your real card or your real bank is not proof it is genuine.
- Never click “verify” or “activate monitoring” links. Open the app or type the address yourself.
- If someone calls “from the fraud team”, hang up and call the number on your card.
- Nobody legitimate asks you to read back a one-time code.

FOR ADMINISTRATORS

- Add mail rules or banners for messages that reference current breaches and external links.
- Watch for new look-alike domains of your bank, payroll and suppliers.
- Treat AI assistants that can read the screen as a data path on managed devices.
- Patch libraries like GPGME inside appliances, not just on servers you build.

FOR BUSINESS LEADERS

- List the suppliers that hold your customers' data, and what each one holds.
- Put breach-notification deadlines in contracts, including your suppliers' own suppliers.
- Prepare a “here is how we will and won't contact you” message now, before you need it.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Which of our suppliers hold customer contact or payment data?
2. How would a customer tell a real notice from us apart from a fake one?
3. Who checks that a payee-change request is genuine before money moves?

Sources

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

[2] SecurityWeek (AP) · 21 Nov 2026 · FBI investigating apparent hack of its key national criminal justice database, AP source says

[3] CNN · 20 Nov 2026 · FBI hacked again, this time targeting crime database

[4] BleepingComputer · 21 Nov 2026 · FBI reportedly hacked again, this time targeting nationwide police database

[5] Forbes · 21 Nov 2026 · FBI reportedly hacked again: apparent breach hits NCIC crime database

[6] FBI · reference · National Crime Information Center (NCIC)

[7] BleepingComputer · 25 Jun 2026 · FBI's CJIS v6.1: what security teams need to know

[8] GnuPG · 20 Nov 2026 · GnuPG Security Advisory for GPGME (T8557, CVE-2026-129975)

[9] GnuPG tracker · 13–20 Nov 2026 · T8557: double free in GPGME read_status / read_colon_line

[10] GnuPG tracker · 20 Nov 2026 · T7659: GPGME 1.24.x legacy branch releases

[11] Debian · 22 Nov 2026 · Security tracker: CVE-2026-129975 (gpgme1.0)

[12] The Hacker News · 21 Nov 2026 · GnuPG warns critical GPGME flaw could expose app data via malicious OpenPGP keys

[13] NebuSec · 20 Nov 2026 · Inside Meta Muse: browser, Sentinel and the shared-kernel boundary

[14] NebuSec · 20 Nov 2026 · Meta Muse credential exposure

[15] The Hacker News · 21 Nov 2026 · A single malicious webpage let researchers hijack Meta Muse and access private chats

[16] Muse (Meta) · Sep 2026 · Security and safety for AI agents: our approach with Muse

[17] Signal · 20 Nov 2026 · Signal is serious about protecting your privacy (Meredith Whittaker)

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

[19] WhatsApp · Nov 2026 · Security advisories 2026: November update

[20] SecurityWeek · 20–21 Nov 2026 · WhatsApp fixes flaw uncovered while disrupting scam campaign

[21] CISA · 20 Nov 2026 · Known Exploited Vulnerabilities catalog, version 2026.11.20 (JSON)

[22] Broadcom · 19–20 Nov 2026 · VMSA-2026-0009.1: VMware vCenter Server and Cloud Foundation updates

[23] Cisco · 21 Oct 2026, v1.0 · Cisco Expressway Series static credential vulnerability (cisco-sa-vcs-static-cred-hr7EWZ8t)

[24] MONAI (GitHub) · 18 Nov 2026 · GHSA-qc22-rmgc-vg94: path traversal in MONAI Label datastore

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

[26] Business Insurance (Reuters) · 20 Nov 2026 · JPMorgan, Visa, Mastercard say third-party vendors targeted in cyberattack

[27] SecurityWeek · 20 Nov 2026 · N-able blames service disruption on cyberattack

[28] The Register · 19 Nov 2026 · Wellington IT breach: Irish credit unions and the six-week gap

[29] The Irish Times · 17 Nov 2026 · Suspected data breach at 43 credit unions could affect hundreds of thousands of members

[30] BleepingComputer · 19 Nov 2026 · Transport for London breach exposes 265,000 Oyster card users' data

[31] Transport for London · Nov 2026 · Cyber security incident

[32] CyberDelegate · 18 Nov 2026 · Rakuten Securities warns customer data from up to 11.25 million accounts may have been exposed

[33] The Record · 20 Nov 2026 · The Container Store restores systems after cyberattack

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

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

[36] The Record · 20 Nov 2026 · NSA resumes normal operations following internal disruptions

[37] BleepingComputer · 18 Nov 2026 · Ukraine, FBI arrest ransomware gang members tied to $40M in ransoms

[38] ransomware.live · 20–22 Nov 2026 · Leak-site claim tracker (claims only, unverified)

[39] SOCRadar · 28 Oct 2026 · n0n ransomware: AI-assisted extortion (background)

HOW WE VERIFIED THIS ISSUE

- Primary sources read: GnuPG's advisory and tracker, the Debian tracker, NebuSec's two write-ups, Signal's blog, WhatsApp's advisory page, the CISA KEV JSON, Broadcom's VMSA and Cisco's advisory.
- The NCIC story rests on anonymous sources reported by CNN and AP; the FBI has not commented. CJIS controls come from a secondary summary and should be read in the policy itself.
- Not reachable: Ubuntu, Red Hat and SUSE trackers, NVD, cisa.gov pages. Leak-site entries are claims only. We left out the National Cyber Director appointment 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 · 22 November 2026
Understand the threat. Build the defense.