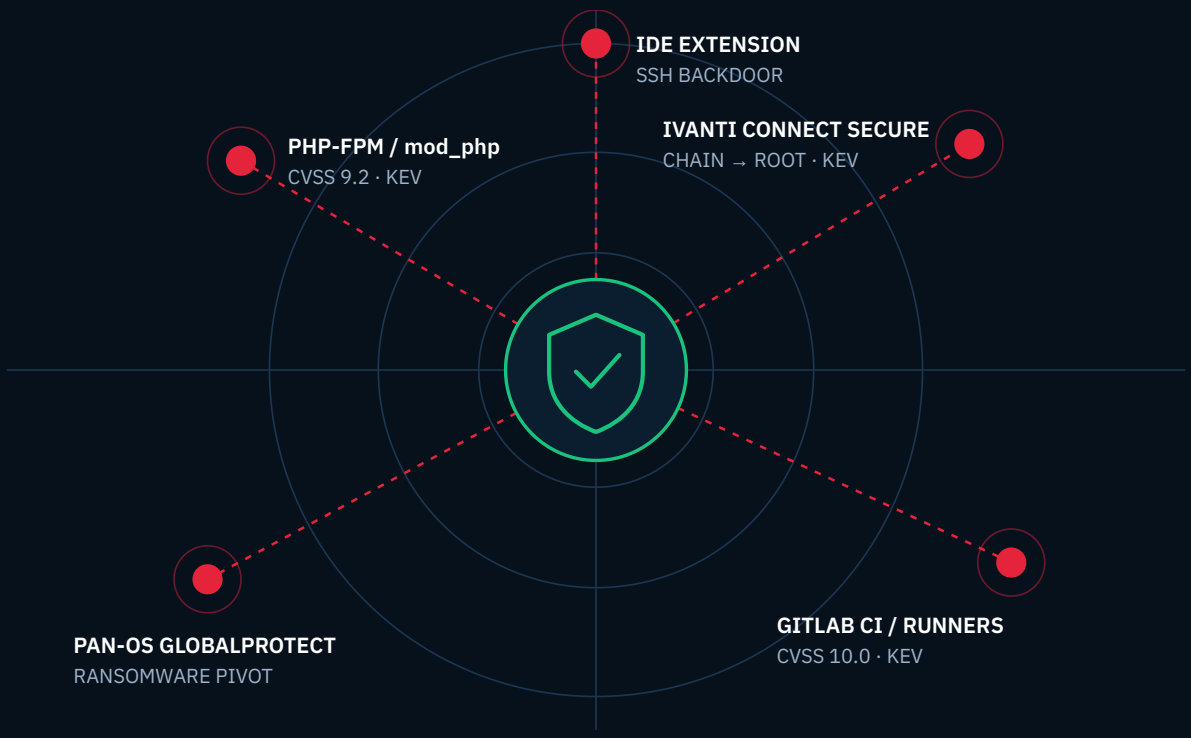
MAG212 CYBER

DAILY INTELLIGENCE

NOVEMBER 1, 2026

EDITION B · PATCH PRESSURE



DEADLINE DAY.

Five exploited footholds, two federal patch deadlines this weekend and one poisoned AI coding extension, with the commands to check every one.

P.03 **PHP2Shell: RCE before your code runs**

P.04 **Ivanti's three-bug chain to root**

P.05 **The extension update that planted SSH keys**

P.06 **GitLab: one regex, CVSS 10**

P.07 **From VPN gateway to hypervisor**

00 / BRIEFING

Today at a glance

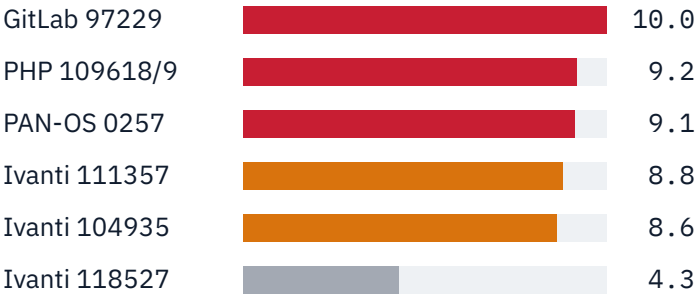
This weekend brings two CISA remediation deadlines, an exploited PHP pair that sits under much of the web, and a trojanized coding extension. Every item below has public evidence of exploitation or malicious delivery.

KEV DEADLINE BOARD · BOD-STYLE TRACKER — as of 01 NOV 2026 07:00 PT

CVE	PRODUCT / FLAW	KEV ADDED	FED DUE	STATUS
CVE-2026-97229	GitLab CE/EE · CI regex integer overflow	29 Oct	01 Nov	DUE TODAY
CVE-2026-111357	Ivanti Connect Secure · privilege escalation	30 Oct	02 Nov	TOMORROW
CVE-2026-118527	Ivanti Connect Secure · predictable filenames	30 Oct	13 Nov	12 DAYS
CVE-2026-109618/9	PHP · OOM corruption + stale-state UAF	26 Oct	29 Oct	PAST DUE
CVE-2026-0257	PAN-OS GlobalProtect · auth bypass	13 May	—	RANSOMWARE

Federal dates apply to US civilian agencies; treat them as an outside limit for everyone else. Sources S2, S5, S10, S11; CVSS per vendor records and S12.

SEVERITY · CVSS BASE SCORE



The lowest score here is still a working link in an exploited chain to root. Exploitation status should set the patch order, not CVSS alone.

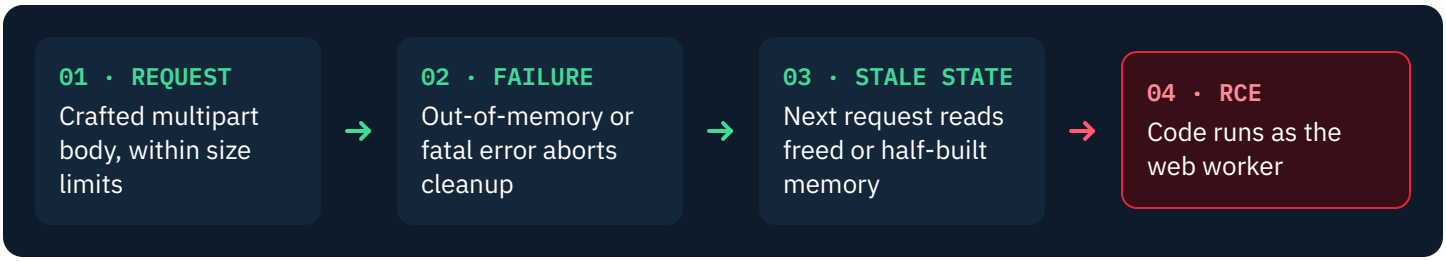
MAG212 PATCH ORDER · THIS WEEKEND

1. **Edge first.** Ivanti to 25.1.1.3 / 22.8R2.6; confirm PAN-OS May fixes. Gateways are the front door.
2. **Internet-facing PHP.** 8.2.35 · 8.3.36 · 8.4.27 · 8.5.12, then restart every worker.
3. **Self-managed GitLab.** 19.5.1 · 19.4.3 · 19.3.6 · 19.2.9 (also fixes CVE-2026-110264), then rotate CI secrets.
4. **Developer laptops.** Hunt for Claude Code 2.1.312/313 from Cursor's marketplace; updating does not clean them.

01 / WEB RUNTIME

PHP2Shell: when a crash path becomes a shell

CVE-2026-109618 + CVE-2026-109619 · CVSS 9.2 each · in CISA KEV since 26 Oct



MAG212 explainer · conceptual flow drawn from the vendor and Rapid7 descriptions, not an exploit reconstruction.

REPORTED FACTS

PHP shipped fixes on 21 Oct. Public proofs of concept appeared on 22 Oct, each tied to one OS, PHP version and web server. CISA added both CVEs to KEV on 26 Oct on evidence of active exploitation. [S1][S2]

WHY IT MATTERS

Under Apache mod_php, 109618 can fire before any application code runs. Researchers also warn that firewall, VPN and ADC web consoles built on PHP share the exposure. [S1][S3]

EXPOSURE BY SAPI

Apache mod_php	HIGHEST
PHP-FPM	CONFIRMED
php-cgi · FrankenPHP	AFFECTED
LiteSpeed	AFFECTED

FIXED RELEASES

8.2.35 · 8.3.36 · 8.4.27 · 8.5.12

8.1 and older: no routine upstream fixes. Check distro backports. [S1]

LINUX / BASH · INVENTORY, THEN INTERIM HARDENING

```
# 1. What is installed and how it is loaded
$ php -v
$ apachectl -M 2>/dev/null | grep -i php
$ dpkg -l 'php*' | grep ^ii   # or: rpm -qa 'php*'

# 2. Current values that matter
$ php -i | grep -E
'memory_limit|post_max_size|upload_progress.enabled'

# 3. Until patched: admin-level FPM pool settings
php_admin_value[session.upload_progress.enabled] = 0
php_admin_value[post_max_size] = 8M
php_admin_value[fatal_error_backtraces] = 0  ; 8.5

$ sudo systemctl restart php8.3-fpm  # all workers
```

MAG212 ANALYSIS

These settings narrow the confirmed paths only. Runtime `ini_set()` and `.user.ini` apply too late. Do not use RLIMIT_AS or cgroup memory caps as a fix: they can trigger the vulnerable allocation-failure path. [S1]

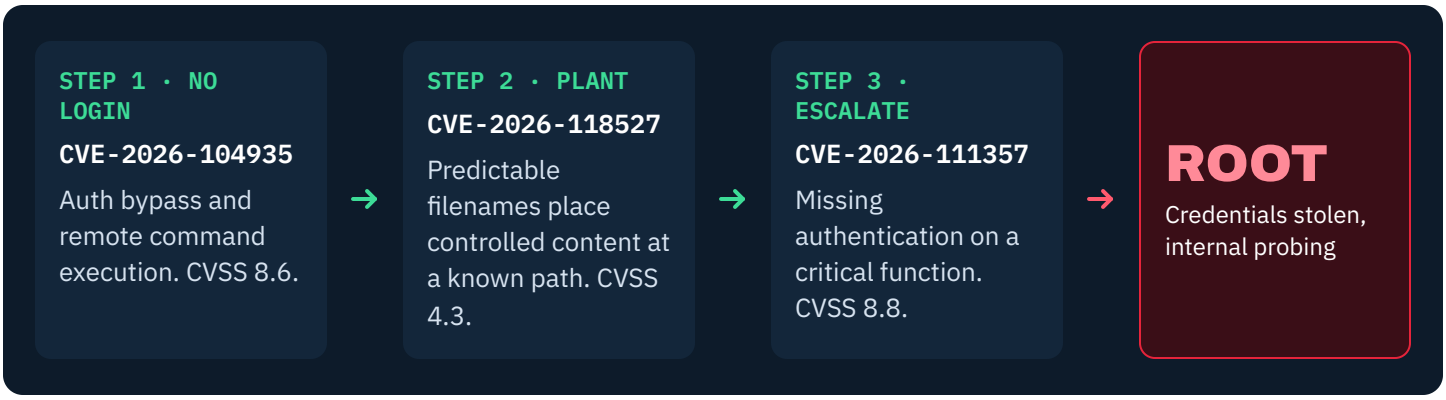
WHAT IS NOT ESTABLISHED

No reliable general-purpose exploit was public as of Rapid7's last update. Quiet logs do not prove safety: suppressing errors does not stop stale-state access. Patching is the only complete fix.

02 / EDGE ACCESS

Three Ivanti bugs, one path to root

Connect Secure · actor UTA0576 (Volexity) · exploited since 3 Oct · federal deadline tomorrow



Chain as described by Ivanti's 29 Oct advisory update and Volexity's analysis. [S4][S6]

TIMELINE

03 OCT
Earliest exploitation Volexity traced

13 OCT
Advisory for 104935; added to KEV

29 OCT
Two more CVEs; 25.1.1.3 and 22.8R2.6 ship

30 OCT
CISA adds both to KEV

02 NOV
Federal deadline for 111357, with forensic triage

VERSION CHECK · CONNECT SECURE

≤ 25.1.1.2	VULNERABLE
22.8R2.5	VULNERABLE
25.1.1.3	FIXED
22.8R2.6	FIXED

The trap: 22.8R2.5 fixed 104935 but is still exposed to the other two. Ivanti lists no workaround; the fix is the upgrade. [S4][S5]

SIEM HUNT · ADAPT FIELD NAMES TO YOUR STACK

```
// Requests to the login CGI carrying the routing
// header Volexity documented in the chain
index=edge_proxy OR index=waf
  uri_path="*/welcome.cgi"
  http_request_headers="*X-DSCGI-PATH*"
| stats count min(_time) max(_time)
        by src_ip, dest_host
| sort - count

// Any hit: preserve logs, run Ivanti's external
// Integrity Checker, then rebuild and rotate creds
```

MAG212 ANALYSIS

A 4.3 score hides a key link. Rank by the chain's outcome, unauthenticated root on the VPN, not by each part. Scanner coverage for the two new CVEs lagged into 31 Oct, so check versions by hand.

WHAT IS NOT ESTABLISHED

Ivanti reports a limited number of affected customers. A clean header hunt does not rule out access before your logs begin.

03 / DEVELOPER SUPPLY CHAIN

The extension update that planted SSH keys

Claude Code 2.1.312 / 2.1.313 via Cursor's marketplace · 29 Oct, 02:27–13:35 PT · up to 5,000 users

EXTENSIONS · anthropic.claude-code	
2.1.312	MALICIOUS
2.1.313	MALICIOUS
2.1.314	CLEAN BUILD

Updating or uninstalling does **not** remove the key, persistence or tunnel. [S8]

SOURCE SCOPE	
Cursor VS Code marketplace	Affected
Microsoft VS Code Marketplace	Not affected
Open VSX · npm · terminal CLI	Not affected

PAYLOAD SEQUENCE · RUNS WHEN THE EDITOR LOADS

01 Loader prepended to `extension.js`; no chat needed

02 Ed25519 key added to `authorized_keys`, comment `svc-telemetry`

03 Tries to enable SSH, installs a startup item

04 Opens a reverse SSH tunnel to the attacker

05 HTTP POST to `/beacon` on port 8099: user, host, public IP, Git email, names of credential env vars

Recon is sent even when the backdoor fails. [S7][S8]

macOS / LINUX · READ-ONLY TRIAGE

```
$ ls -d ~/.cursor/extensions/\
    anthropic.claude-code-2.1.31[23]*
$ grep -n svc-telemetry \
    ~/.ssh/authorized_keys
$ ls -lt ~/Library/LaunchAgents | head
$ sudo systemsetup -getremotelogin
$ lsof -nP -i | grep ':8099'
```

WINDOWS / POWERSHELL · READ-ONLY

```
PS> gci "$env:USERPROFILE\.cursor\
     extensions" -Filter *claude-code-2.1.31*
PS> sls svc-telemetry `
     "$env:USERPROFILE\.ssh\authorized_keys"
PS> Get-Service sshd -EA 0
PS> Get-NetTCPConnection -RemotePort 8099 `
     -EA 0
```

Checks are MAG212 proposals built from published indicators. Paths can differ by editor; Cursor's own impact check and remediation scripts take precedence. [S7]

MAG212 ANALYSIS

The attacker shipped under the real extension ID, so name-based allowlists passed it. Anthropic says it did not build or publish the copy; how the marketplace was accessed is undisclosed. Watch behavior: an editor plugin writing SSH keys should alert in seconds.

IF YOU FIND IT

Isolate the host. Remove the key, startup item and tunnel. Rotate the Git, cloud and API secrets named in the beacon. Consider a rebuild. Cursor notes that enabling SSH needs admin rights the extension lacked on most hosts.

04 / CI/CD PLATFORMS

GitLab: one regular expression, CVSS 10

CVE-2026-97229 · self-managed CE/EE · in KEV since 29 Oct · federal deadline is today



Illustrative only: the pattern placeholder is not a working payload. Mechanism per GitLab's advisory as reported. [S10]

REPORTED FACTS

GitLab fixed the flaw on 12 Oct. On 20–21 Oct an attacker sent crafted CI configs to Alpine Linux's unpatched instance, crashed eight workers and pulled the GitLab container image. Alpine rebuilt. Later attempts on 25–26 Oct were blocked. [S10]

MAG212 ANALYSIS

A CI server holds the keys to production: variables, runner tokens, deploy keys and cloud credentials. If you were unpatched and exposed in late October, treat secret rotation as part of the patch, not a follow-up.

ADMIN › HELP · VERSION

19.5 line	≥ 19.5.1
19.4 line	≥ 19.4.3
19.3 line	≥ 19.3.6
19.2 line	≥ 19.2.9

The 12 Oct builds fix 97229 but not CVE-2026-110264 (CVSS 10, fixed 21 Oct). Older lines: 19.1.9 · 19.0.10 · 18.11.13. [S10][S16]

OMNIBUS / BASH · VERIFY, BACK UP, THEN HUNT

```
$ sudo gitlab-rake gitlab:env:info | grep -A2 '^GitLab information'
$ sudo gitlab-backup create        # copy the archive off-host before upgrading

# Worker crashes during the unpatched window (regex engine is Onigmo)
$ sudo grep -ril onigmo /var/log/gitlab/ | head

# Admins and runners created in the last 30 days
$ sudo gitlab-rails runner 'p User.admins.where("created_at > ?", 30.days.ago).pluck(:username)'
$ sudo gitlab-rails runner 'p Ci::Runner.where("created_at > ?", 30.days.ago).pluck(:id)'
```

PATCH
Go straight to the 21 Oct releases; plan downtime for migrations.

ROTATE
CI variables, deploy keys, runner tokens, cloud creds.

RESTRICT
Keep self-managed GitLab behind a VPN where possible.

REBUILD
Anything suspicious: restore from a known-good backup.

05 / RANSOMWARE TRADECRAFT

From VPN gateway to hypervisor

PAN-OS GlobalProtect CVE-2026-0257 · fixed since May · now used by Qilin and Inc operators

OBSERVED INTRUSION PATH · UNIT 42

01 EDGE
Auth bypass on GlobalProtect; MFA skipped

→

02 RECON
Dual-use RMM tools inside the VPN

→

03 LATERAL
RDP and SMB; Veeam CVE-2023-27532 chained

04 vCENTER
Pivot to the management appliance

→

05 ESXi
execInstalledOnly turned off

→

06 CREDENTIALS
DC's VMDK dumped offline, out of EDR's view

REPORTED FACTS

Unit 42's 19 Oct update links the flaw to Spikey Scorpius (Qilin) and Tarnished Scorpius (Inc). Fixes shipped in May; attempts hit unpatched gateways without mitigations. [S11]

MAG212 ANALYSIS

Reading a domain controller's disk from the hypervisor skips every in-guest control. Treat vCenter and ESXi as tier-0 assets, equal to the DC itself.

MONITOR › LOGS › GLOBALPROTECT · FILTER: PoC FINGERPRINT — illustrative view

EVENT	DEVICE NAME	CLIENT OS	SRC USER DOMAIN
gateway-connected	DESKTOP-GP01	Windows 10 Pro 64-bit	(empty)
gateway-connected	GP-CLIENT	Windows 10 Pro 64-bit	(empty)
gateway-connected	WINDOWS-LAPTOP-001	Windows 10 Pro 64-bit	(empty)

Also published: host IDs aa:bb:cc:dd:ee:ff, 00:11:22:33:44:55 and nine source IPs. Any match: start IR. [S11]

PAN-OS CLI · READ-ONLY

```
> show system info | match sw-version
> show global-protect-gateway
    current-user
# compare with the fixed release in
# the vendor advisory for your train
```

ESXi SHELL · CHECK THE GUARDRAIL

```
# esxcli system settings kernel list \
    -o execInstalledOnly
# Configured/Runtime should be TRUE.
# FALSE you did not set = investigate.
```

Hardening from Unit 42: use a dedicated certificate for Authentication Override cookies, or turn Authentication Override off on portal and gateway. Confirm ports 4443 and 3879 on the management IP are not reachable from outside.

ALSO ON THE RADAR

AI · OPEN WEIGHTS

Mistral Large 4 goes open-weight

A trillion-parameter multimodal model aimed at software and defensive security teams who want it on their own hardware. [S13]

AI · SECURITY MODELS

DeepSeek V4.1 Flash Cyber

A security-tuned variant released 29 Oct. Treat claims as unverified until independent evaluations land. [S14]

WINDOWS · PATCH BACKLOG

October's record Patch Tuesday

1,413 CVEs, including exploited Shell bypass CVE-2026-96951. Confirm rollout before November's cycle. [S15]

Covered in Edition A today: LXD/MicroCloud auth bypass, the Polymarket script compromise, the Binance theft and NetamLoader.

SOURCES · CHECKED 01 NOV 2026

S1 Rapid7 · PHP CVE-2026-109618/9 analysis · rapid7.com

S2 runZero · PHP KEV update, 27 Oct · runzero.com

S3 BleepingComputer · InfraTrust report on appliances · bleepingcomputer.com

S4 Ivanti · Connect Secure advisory, rev. 29 Oct · hub.ivanti.com

S5 CISA · Two KEV additions, 30 Oct · cisa.gov

S6 GBHackers · Volexity UTA0576 findings · gbhackers.com

S7 BleepingComputer · Cursor notice on Claude Code ext. · bleepingcomputer.com

S8 Phorion · Extension compromise advisory · phorion.io

S9 StepSecurity · Trojanized 2.1.312/313 builds · stepsecurity.io

S10 The Back Room Tech · GitLab CVE-2026-97229 · thebackroomtech.com

S11 Unit 42 · PAN-OS CVE-2026-0257, upd. 20 Oct · paloaltonetworks.com

S12 Senserva · KEV weekly tracker (CVSS) · senserva.com

S13 The Neuron · AI digest, 30 Oct · theneuron.ai

S14 LLM Gateway · Model release timeline · llmgateway.io

S15 Tech Times · Patch Tuesday, October 2026 · techtimes.com

S16 IT-Connect · GitLab CVE-2026-110264, 21 Oct fixes · it-connect.tech

REPORTING METHOD

Facts come from vendor advisories, CISA and named research teams, with secondary reporting used where primary pages were unavailable. Analysis is labelled MAG212. Commands are proposed read-only checks, not tests run by MAG212 on affected systems.

LIMITATIONS

Diagrams are conceptual, not victim-network reconstructions. Console panels are illustrative layouts. Incident counts and versions can change; check the vendor before you act.

MAG212 CYBER
UNDERSTAND THE THREAT. BUILD THE DEFENSE.
Subscribe free
cyber.mag212.com/subscribe-free/