

MAG212CYBER

DAILY CYBER MAGAZINE SPECIAL EDITION FRIDAY · OCTOBER 30, 2026

ISSUE 2026-303

🔥 LEAD STORY · NATION-STATE

THE \$6.36B HEIST

North Korea's TraderTraitor is linked to the largest crypto theft ever. Ten chains, twenty minutes, and an Ethereum feature turned into a skeleton key. [Page 03](#)

\$8.9B+

CRYPTO STOLEN
IN 24 HOURS

4

CVES IN
THIS ISSUE

3

EXPLOITED
IN THE WILD

NOV 1

KEV FEDERAL
DEADLINE

ALSO IN THIS ISSUE

SUPPLY CHAIN

One poisoned RUM script drains \$2.6M from Polymarket

p.04

CVE-2026-97229

GitLab RCE scores 10.0 and nearly lands on Alpine Linux

p.05

CVE-2026-76418

Cisco ASA/FTD VPN crash bug added to CISA's KEV catalog

p.06

CVE-2026-111585

TeamViewer: when the customer's host attacks the tech

p.07

CVE-2026-118539

Drupal Commerce access bypass under active attack

p.08

THREAT
BRIEFING

DETECTION
LAB

45-MIN BLUE-TEAM
WORKSHOP

INCIDENT RESPONSE
CHECKLIST

cyber.mag212.com

THREAT BRIEFING

Today's threat board

Six incidents, four CVEs, three confirmed exploited. Every ID, score and version below was re-checked against vendor advisories, the CVE record or the original reporting on Oct 30, 2026.

\$6.36B

BINANCE STOLEN (TRM)

≈\$2.5-3B

FROZEN BY ISSUERS

~700

POLYMARKET
ACCOUNTS HIT

10.0

TOP CVSS THIS ISSUE

3 days

KEV DEADLINE WINDOW

INCIDENT	ID	SEVERITY	EXPLOITED	FIX / ACTION	PG
Binance hot-wallet theft	—	No CVE	Actor: TraderTraitor (assessed)	Freeze, re-key signers	03
Polymarket RUM script	—	Supply chain	Yes · Oct 29	Remove script · SRI · CSP	04
GitLab / Ruby Onigmo	CVE-2026-97229	10.0	Yes · KEV	19.5.1+ / Ruby 3.3.13+	05
Cisco ASA / FTD RA-VPN	CVE-2026-76418	8.6	Yes · KEV	Fixed train / disable 2nd auth	06
TeamViewer viewer	CVE-2026-111585	8.8	Not known	15.83 / legacy builds	07
Drupal Commerce Core	CVE-2026-118539	21/25	Yes (Drupal)	3.3.13 / 8.x-2.41	08

🕒 HOW THE WEEK UNFOLDED

● Oct 12

GitLab 19.4.2 / 19.3.5 / 19.2.8 fix CVE-2026-97229

● Oct 20

Attacker registers an account on Alpine's GitLab

● Oct 21

8 worker crashes at Alpine; exploit fails mid-chain

● Oct 23

oss-security: Regexp.timeout doesn't mitigate Onigmo bugs

● Oct 27

TeamViewer TV-2026-1011 published

● Oct 28

Cisco advisory · Drupal SA-CONTRIB-2026-254 · Alpine post

● Oct 29

Polymarket drained 17:10 UTC · Binance drained 20:05 UTC

● Oct 29

CISA adds GitLab + Cisco flaws to KEV

● Nov 1

KEV federal remediation due (per THN)

⚠️ PATCH PRIORITY LADDER

P1 · TODAY

Internet-facing GitLab and Drupal Commerce: both exploited, both reachable by strangers.

P1 · TODAY

Any third-party JS on pages that handle money or sessions: inventory, pin and set CSP.

P2 · 48 H

Cisco ASA/FTD with webvpn + secondary auth: patch or mitigate before Nov 1.

P3 · THIS WEEK

TeamViewer viewers across help desk and MSP fleets, including portable copies.

ONGOING

Crypto and fintech: signer policy, EIP-7702 monitoring, developer-lure awareness.

📞 MITRE ATT&CK MAPPING

T1195.002	Compromise Software Supply Chain	Polymarket
T1059.007	JavaScript execution	Polymarket
T1190	Exploit Public-Facing Application	GitLab · Drupal
T1136	Create Account	GitLab / Alpine
T1499.004	Endpoint DoS: Application Exploitation	Cisco
T1203	Exploitation for Client Execution	TeamViewer
T1566	Phishing (lures, assessed TTP)	TraderTraitor
T1657	Financial Theft	Binance · Polymarket

Editorial mapping by MAG212 CYBER, not vendor-supplied.

📄 EDITOR'S NOTE

Thursday showed how much trust each part of the stack carries. A monitoring script was trusted with wallets. A regex engine was trusted with user input. A support viewer was trusted to render a stranger's screen. A hot-wallet signer was trusted to sign whatever it was handed.

The common fix isn't a product. Know what runs in your trust boundary, pin it, and log what leaves it. Alpine could prove its packages were clean because its signing keys lived somewhere else. That habit is worth copying.

— El Mostafa Ouchen, MAG212 CYBER

TRM LABS · CHAINALYSIS · SECURITYWEEK

NATION-STATE · CRYPTO

HIGH-CONFIDENCE ATTRIBUTION

ROOT CAUSE UNPUBLISHED

\$6.36 Billion Binance Heist Bears the Hallmarks of North Korea's TraderTraitor

On Oct 29, 2026 attackers emptied Binance hot wallets across ten chains in roughly twenty minutes, making it the largest crypto theft on record. Blockchain-intelligence firms TRM Labs and Chainalysis both attribute it to the DPRK cluster tracked as TraderTraitor with high confidence. Binance has not confirmed the attribution or published a root cause.



\$6.36B

stolen at time of theft (TRM)

DETECTED	Oct 29 · 20:05 UTC; second wave 23:05 UTC
CHAINS	10 · ETH, Tron, BTC and others
ESTIMATES	TRM \$6.36B · Binance ≈\$6.3B · Chainalysis ≥\$5.91B
FROZEN	≈\$2.5–3B (Tether ≈1.77B USDT, Circle 823M USDC)
ACTOR	TraderTraitor · a.k.a. Jade Sleet / UNC4899 / Slow Pisces
STATUS	Laundering in progress

ATTACK CHAIN



1

Pre-staging

Operator wallet funded via Tornado Cash the day before; test runs



2

Signer access

Attacker can get Binance's hot-wallet signing system to sign (TRM)



3

50 pre-signed auths

EIP-7702 delegation hands an ETH hot wallet to a sweeper contract



4

Burst drain

Signed transfers on other chains; most funds out in ~20 min



5

Laundering

UniswapX swaps to ETH, Aave borrow, JustLend, BTC peel chain

01 HOW IT HAPPENED



Signing infrastructure, not one key. TRM's assessment is that the attacker could make the exchange's hot-wallet signing service sign arbitrary transactions.



EIP-7702 abuse. 50 pre-signed authorizations delegated an Ethereum hot wallet's code to an attacker sweeper contract, which then pulled assets.



Initial access unconfirmed. Early reporting cites a compromised engineer laptop leading to a service container. Binance has not confirmed this.



Fired in one burst. Signatures were collected in advance and executed together, leaving almost no time to react.

02 HOW YOU'D KNOW YOU WERE HIT



Type-0x04 transactions (EIP-7702 SetCode) touching treasury or hot-wallet EOAs you never meant to delegate.



Signer anomalies: signing requests outside policy windows, unusual batch sizes or destinations not on allowlists.



Tornado-funded gas wallets interacting with your contracts in the 24–48 h before an event.



Developer-endpoint alerts: fake job-offer or 'coding test' lures, trojanised npm/PyPI packages, odd container access.

03 HOW TO REMEDIATE



Freeze and coordinate fast. Stablecoin issuers froze ~\$2.5–3B here; pre-arranged contacts with Tether, Circle and analytics firms matter.



Re-key the signer. Rotate MPC/HSM key shares and API credentials; rebuild signing hosts from known-good images.



Kill stale authorizations. Revoke or overwrite any EIP-7702 delegations; refuse pre-signed payloads that outlive their session.



Rebuild developer access. Reimage engineer laptops in scope, rotate cloud and CI secrets, re-verify container images.

04 DEFENDER NOTES



Policy at the signer. Enforce per-transaction and per-window value limits, destination allowlists and time locks inside the signing service itself.



Hunt for the lure. TraderTraitor has long targeted crypto staff with job-themed social engineering (FBI PSA, Feb 2025, on Bybit).



Treat 'frozen' ≠ 'recovered'. On TRM's figures, \$3.4–3.7B is likely unrecoverable even after freezes.

eth-watch.js · flag EIP-7702 delegations on hot wallets (ethers v6)

```
const HOT = new Set(['0xYourHotWallet1', '0xYourHotWallet2'].map(a => a.toLowerCase()));
provider.on('block', async (n) => {
  const b = await provider.getBlock(n, true);
  for (const tx of b.prefetchedTransactions) {
    if (tx.type !== 4) continue; // 0x04 = EIP-7702 SetCode
    for (const au of tx.authorizationList ?? []) {
      const who = ethers.verifyAuthorization(au, au.signature).toLowerCase();
      if (HOT.has(who)) page(`7702 delegation: ${who} -> ${au.address}`);
    }
  }
});
```

WHAT WE STILL DON'T KNOW

- Binance's root cause and the exact signer weakness
- Attacker addresses: none published
- TRM cites "420,000+ ETH" held, but only ~228.6K ETH was stolen directly. The gap is unreconciled
- Ripple's claimed ~\$200M assist; TRM confirms a 40.5M RLUSD freeze only

SECURITYWEEK · GOPLUS · DEBUGBEAR

WEB SUPPLY CHAIN

THIRD-PARTY JS

REFUNDS PLEDGED

\$2.6M+ Drained From Polymarket Traders Through a Poisoned Monitoring Script

A real-user-monitoring (RUM) script served from performance vendor DebugBear's CDN was swapped for about 15 KB of wallet-drainer code. For roughly an hour on Oct 29 it ran inside Polymarket's international site, read session secrets from the browser and emptied about 700 accounts.

HIGH

NO CVE

~700

accounts hit · 710 deposit wallets

VECTOR	Compromised vendor-hosted RUM script
FILE	cdn.debugbear[.]com/C7xcKKrjUnXK.js
LOSS	≈\$2.6–2.71M (SecurityWeek: "\$2M+")
WINDOW	≈17:10–17:59 UTC, Oct 29
DRAIN ADDR	0x3F99...Ffc18
SCOPE	International site only · trading halted ≈1 h

ATTACK CHAIN



1

Vendor CDN hit

DebugBear-hosted RUM file replaced (breach method undisclosed)



2

Drainer loads

~15 KB JS runs in Polymarket's origin for every visitor



3

Secrets read

Login data, deposit address and trading API creds from browser storage



4

React hijack

Walks the component tree to grab the live trading client and signer



5

Sweep

Fill-and-kill sells, then funds swept to one attacker address

01 HOW IT HAPPENED

- Same-origin trust.** A third-party script loaded into the page inherits full access to the DOM and storage. The drainer needed no exploit.
- Email/Magic accounts:** the script signed silently with the embedded signer, dumped positions with fill-and-kill sell orders and swept the proceeds.
- External-wallet users:** it built batch ERC-1155 outcome-token transfers via the gasless relay. Those raised signature prompts, and some users approved them.
- Fast detection.** A trader flagged an ~\$800K loss at 17:46 UTC; the script was removed in commit #15337 at 17:59.

02 HOW YOU'D KNOW YOU WERE HIT

- Script hash drift:** a vendor file changes size or hash with no release note. Here it ballooned to ~15 KB.
- New fetch targets** in CSP violation reports, RUM beacons or browser network logs.
- Unexpected sells/transfers** clustered in time across many unrelated accounts.
- Unusual signature prompts** for batch token transfers that users didn't initiate.

03 HOW TO REMEDIATE

- Pull the tag first.** Remove the third-party script, purge CDN and edge caches, then investigate.
- Invalidate everything client-side.** Revoke sessions and trading API keys; force re-auth so stolen tokens die.
- Scope from the chain.** Map the drain address on-chain to enumerate affected wallets and amounts.
- Communicate and make whole.** Polymarket paused trading, pledged full refunds and referred the case to UK police.

04 DEFENDER NOTES

- Pin with SRI or self-host.** Subresource Integrity breaks loudly if the vendor file changes; self-hosting removes the vendor CDN from your trust path.
- Never keep keys where scripts can reach.** Trading credentials in localStorage are readable by any script on the page.
- Don't merge incidents.** This is distinct from Polymarket's June 2026 vendor breach (~\$3M pUSD).

THE TAKEAWAY Every script on a money page holds the keys. Pin it, or own it.

● ● ● sri-pin.sh · compute an SRI hash and pin the vendor script

```
# 1. hash the reviewed copy of the vendor file
openssl dgst -sha384 -binary rum.js | openssl base64 -A

# 2. load it with integrity + CORS, so any change fails closed
<script src="https://cdn.vendor.example/rum.js"
  integrity="sha384-<hash-from-step-1>" crossorigin="anonymous"></script>

# 3. CSP: allow only named origins, report the rest
Content-Security-Policy: script-src 'self' https://cdn.vendor.example;
connect-src 'self' https://api.example.com; report-to csp-endpoint
```

🕒 TIMELINE · OCT 29 (UTC)

- 17:10** first funds reach attacker
- 17:46** trader reports ~\$800K loss
- 17:59** "remove debugbear rum script (#15337)"
- 18:20** attacker holds 28.6M POL ≈ \$2.64M

DebugBear confirmed an incident and told customers to remove its RUM snippet. How its CDN was breached is not yet public.

SECURITYWEEK · ALPINE LINUX · GITLAB

DEVSECOPS · RCE

CISA KEV

EXPLOITED

CVSS 10.0

Max-Severity GitLab Flaw CVE-2026-97229 Turned Against Alpine Linux

A crafted regular expression in CI/CD configuration triggers an integer overflow in Onigmo, the regex engine inside Ruby, giving unauthenticated remote code execution. Alpine's GitLab was one patch behind. The attack crashed workers eight times and, in Alpine's words, "came close to working."

10.0

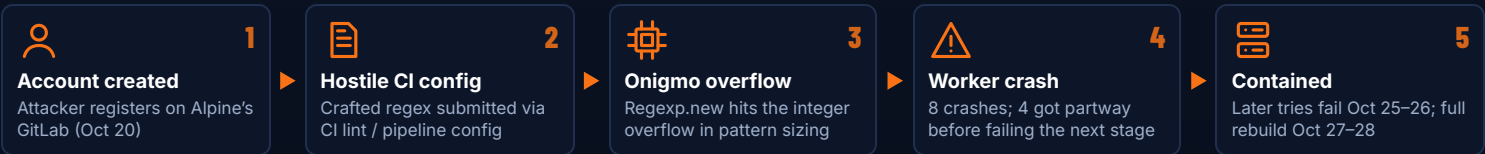
CVSS 3.1

8x

worker crashes at Alpine on Oct 21

CVE	CVE-2026-97229 · related CVE-2026-110264 (10.0)
VECTOR	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
ROOT CAUSE	Onigmo compiled-pattern size overflow (Ruby #19020)
FIXED	GitLab 19.4.2 / 19.3.5 / 19.2.8 (Oct 12)
LATEST	19.5.1 · 19.4.3 · 19.3.6 · 19.2.9 · 19.1.9 · 19.0.10 · 18.11.13
RUBY	3.3.13 · 3.4.12 · 4.0.9 (3.2: no fix)

ATTACK CHAIN



01 HOW IT HAPPENED

- Version drift.** Alpine ran GitLab 19.3.4, not the fixed 19.3.5, by mistake.
- Fix lives in Ruby.** GitLab ships the fix as a patched Ruby inside its official packages. Alpine's image used stock Ruby, so upgrading GitLab to 19.3.6 alone did not close it.
- User-controlled regex.** GitLab compiles patterns from CI configuration with Regexp.new, putting a memory-corruption bug one YAML file away.
- Reported by** Johan Carlsson ("joaxcar") via GitLab's HackerOne programme.

02 HOW YOU'D KNOW YOU WERE HIT

- Puma/Workhorse crashes, 502s** and failed CI jobs clustered around CI-lint requests.
- Fresh accounts** submitting CI config or calling ci/lint (REST or GraphQL) soon after sign-up.
- GitLab's six detections:** Onigmo native worker crash · GraphQL cilint hostile regexp · ci regexp oversized non-ASCII path · ci regexp guard rejection · ci lint workhorse worker crash · ci lint scripted client error burst.
- Big caveat:** a successful exploit leaves no crash and no web-log trace. Crash-based detection catches failures only.

03 HOW TO REMEDIATE

- Upgrade to the latest patch** (19.5.1, 19.4.3, 19.3.6 ...), which also covers CVE-2026-110264 (GitLab 7.0+).
- Custom/source installs:** also upgrade Ruby to 3.3.13, 3.4.12 or 4.0.9+. Ruby 3.2 has no fix, so move off it.
- Limit who can register.** Require admin approval or disable open sign-up on self-managed instances.
- If in doubt, rebuild.** Alpine rebuilt from scratch, reset all passwords and rotated GitLab secret keys.

04 DEFENDER NOTES

- Regexp.timeout won't save you.** These are memory bugs, not ReDoS; pattern-length limits are unreliable too (oss-security).
- Separate signing from forge.** Alpine's signing keys were never on the GitLab host, which is why its packages and releases stayed trustworthy.
- Log egress.** Alpine could not rule out success partly because outbound connections weren't logged.

gitlab-check.sh · confirm both GitLab and the Ruby it actually runs

```
# Omnibus / Linux package
sudo cat /opt/gitlab/embedded/service/gitlab-rails/VERSION
/opt/gitlab/embedded/bin/ruby -v          # GitLab-patched Ruby
sudo gitlab-rake gitlab:env:info | grep -E 'GitLab information|Version|Ruby'

# Source / container builds: the runtime Ruby is what matters
ruby -v          # need >= 3.3.13 | 3.4.12 | 4.0.9 (3.2.x: unsupported)

# Hunt failed attempts: worker deaths near CI lint calls
sudo grep -E 'ci/lint|ciConfig' /var/log/gitlab/gitlab-rails/production_json.log | tail
sudo grep -iE 'SIGSEGV|worker.*(died|terminated)' /var/log/gitlab/puma/puma_stderr.log
```

WHAT ALPINE VERIFIED

- aports and binary packages untampered
- Oct 21 releases 3.21.9 · 3.22.7 · 3.23.7 · 3.24.3 clean
- Signing keys never on the GitLab server
- No evidence of code execution, but it can't be ruled out

GitLab rates this unauthenticated, yet the attacker registered an account first. Alpine didn't say why.

CISCO PSIRT · THE HACKER NEWS · CISA

NETWORK EDGE · DOS

CISA KEV

EXPLOITED

DOS, NOT RCE

Cisco ASA & FTD Remote-Access VPN Crash Flaw CVE-2026-76418 Exploited in the Wild

An unauthenticated, crafted request to the Remote Access SSL VPN login service forces affected firewalls to reload. Exposure needs a specific configuration: secondary authentication on a tunnel group. Cisco confirmed exploitation in October 2026, and CISA added the flaw to its Known Exploited Vulnerabilities (KEV) catalog on Oct 29.

8.6

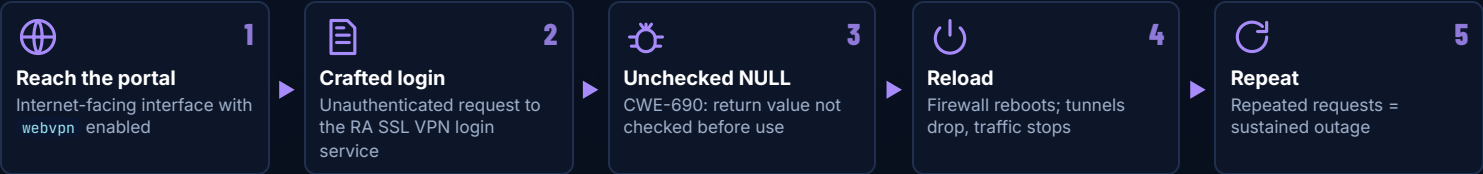
CVSS 3.1

0

workarounds · mitigation only

ADVISORY	cisco-sa-asaftd-tunnel-dos-s6mgkb75
BUG / CWE	CSCwx26625 · CWE-690
VECTOR	AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
PUBLISHED	Oct 28, 2026 · credit: Eric Fernald (TAC case)
KEV	Added Oct 29 · federal due Nov 1 (per THN)
IMPACT	Device reload: VPN and traffic outage

ATTACK CHAIN



01 HOW IT HAPPENED

- Two preconditions. webvpn enabled on an interface and a tunnel group (including DefaultWEBVPNGroup) with secondary-authentication-server-group set.
- Availability only. Cisco scores C:N/I:N/A:H. There is no confidentiality or integrity impact, and this is not a code-execution flaw.
- Found in support. Surfaced during a Cisco TAC case by Eric Fernald.

02 HOW YOU'D KNOW YOU WERE HIT

- Unexplained reloads on devices matching both preconditions. This is the only symptom Cisco names.
- New crashinfo files and 'last reload reason' entries that don't match change records.
- VPN user spikes of disconnects and helpdesk tickets at the time of reloads.
- No IOCs published: Cisco lists no syslog IDs or crash signatures, so correlate timing yourself.

03 HOW TO REMEDIATE

- ASA fixed: 9.16.4.104 · 9.18.4.96 · 9.20.4.50 · 9.22.3.200 · 9.23.1.48 · 9.24.1.27 / 9.24.10.1
- FTD fixed: 7.0.11 · 7.2.13 · 7.4.9 · 7.6.7 · 7.7.14 · 10.0.3 · 10.1.1
- Mitigate until patched: no secondary-authentication-server-group or no tunnel-group-list enable, after checking the impact on logins.
- Before changes: save config and crashinfo; plan HA failover and a maintenance window.

04 DEFENDER NOTES

- Don't conflate. A separate ASA/FTD VPN DoS was reported exploited in August 2026; verify which advisory you're patching.
- Edge devices are crown jewels. Repeated DoS can mask or precede other activity. Keep off-box syslog.

THE TAKEAWAY

A firewall that reboots on demand is an outage you don't control. If you can't patch before Nov 1, turn off secondary auth and watch reload reasons.

asa-exposure.txt · am I in scope? (ASA CLI)

```
show version | include Version|reload
show running-config webvpn          ! enable <ifname> present?
show running-config tunnel-group | include secondary-authentication-server-group
show crashinfo | include Thread|Traceback      ! recent crash?

! temporary mitigation (test the impact on 2FA logins first)
tunnel-group <NAME> general-attributes
no secondary-authentication-server-group
```

KEY DEADLINE

NOV 1

The Hacker News reports a three-day federal due date. That is unusually short (normally ~21 days), so confirm it in CISA's catalog.

TEAMVIEWER TV-2026-1011 · SECURITYWEEK

REMOTE ACCESS · CLIENT-SIDE

NOT EXPLOITED (YET)

REVERSE ATTACK

TeamViewer Flaw CVE-2026-111585 Lets a Malicious Host Attack the Technician

Remote support normally trusts the technician's side. Here the risk runs the other way. An integer overflow in the viewer's screen-decompression code can cause a heap overflow when a malicious or compromised host sends crafted screen data, crashing the viewer or, on some platforms, running code as the technician.



15.83

fixed build · Win · macOS · Linux · Android

BULLETIN TV-2026-1011 · Oct 27 (upd. Oct 28)

VECTOR AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE CWE-190 → heap buffer overflow

CREDIT Omri Dar (per CVE record)

SIBLINGS CVE-2026-92372 (8.8) · CVE-2026-92374 (7.8)

STATUS No known exploitation · no public PoC

ATTACK CHAIN



1

Lure

Technician is asked to connect to a 'customer' host



2

Session opens

Technician initiates the session (UI:R)



3

Crafted frames

Host streams malformed compressed screen data



4

Int overflow

Size wraps → undersized buffer → heap overflow



5

Viewer owned

Crash, or code execution with the viewer's privileges

01 HOW IT HAPPENED

- Trust inverted.** Help desks and MSPs connect to untrusted endpoints all day. A compromised customer machine becomes a weapon against the support desk.
- CWE-190 → heap overflow.** A size calculation in the remote-control screen-processing path overflows, so decompressed data overruns its buffer.
- Sibling bug, CVE-2026-92372:** an out-of-bounds write in the image decoder on Linux/macOS, also reachable by opening a crafted .tvs session recording.
- CVE-2026-92374:** a separate macOS local privilege escalation to root.

02 HOW YOU'D KNOW YOU WERE HIT

- Viewer crashes** that coincide with a session to a specific host, especially repeatable ones.
- Odd child processes** spawned by TeamViewer.exe / TeamViewer (shells, script hosts, LOLBins).
- .tvs recordings** received from outside parties and opened on Linux/macOS.
- Note:** TeamViewer published no indicators. These hunts are our editorial suggestions.

03 HOW TO REMEDIATE

- Update every viewer** to 15.83 (Full Client, Portable, Android Remote Control).
- Legacy branches:** 15.64.10 (Win 7/8) · 14.7.48868 · 13.2.36231 (Win) · 13.2.154008 (Linux) · 13.2.154007 (macOS).
- Find portable copies.** Portable builds escape software inventory, so hunt by file name and hash.
- No workaround.** TeamViewer offers patching only.

04 DEFENDER NOTES

- Least privilege for techs.** Run support consoles as standard users on hardened, segmented machines so a viewer compromise isn't a domain compromise.
- Version mismatch.** Canada's Cyber Centre (AV26-1093) lists Android 15.8.3; TeamViewer lists 15.83. Go by the vendor.

THE TAKEAWAY

Remote support is a two-way trust. The screen you're viewing can attack you, so patch every viewer and keep technicians on least-privilege machines.

tv-version · find vulnerable viewers

```
# Windows (PowerShell)
Get-ItemProperty HKLM:\SOFTWARE\TeamViewer, HKLM:\SOFTWARE\WOW6432Node\TeamViewer `
-ErrorAction SilentlyContinue | Select-Object Version
Get-ChildItem C:\Users\*\Downloads\TeamViewer*.exe -ErrorAction SilentlyContinue # portable

# macOS
defaults read /Applications/TeamViewer.app/Contents/Info.plist CFBundleShortVersionString

# Linux
teamviewer --version
```

WHO SHOULD CARE MOST

- MSPs and outsourced help desks
- Internal IT supporting BYOD or contractors
- Anyone who opens .tvs recordings from third parties

DRUPAL SA-CONTRIB-2026-254 · THE HACKER NEWS

E-COMMERCE · ACCESS BYPASS

HIGHLY CRITICAL 21/25

EXPLOITED

Highly Critical Drupal Commerce Access Bypass CVE-2026-118539 Under Active Attack

Drupal's security team says some Commerce Core routes and entity fields are not properly protected, an access bypass that "may financially impact the vendor." Drupal reports active exploitation. Stores on 8.x-2.x below 2.41 or 3.x below 3.3.13 should patch now and audit their orders.

21

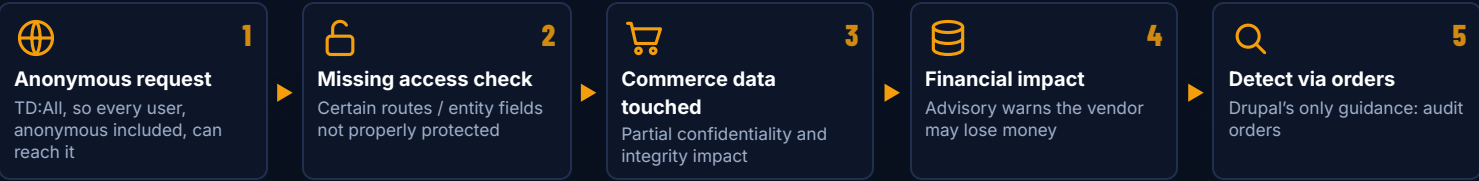
OF 25 · DRUPAL

21/25

Drupal risk score · Highly critical

ADVISORY	SA-CONTRIB-2026-254 · Oct 28, 2026
RISK	AC:None/A:None/CI:Some/II:Some/E:Exploit/TD:ALL
AFFECTED	< 8.x-2.41 · 3.0.0 to < 3.3.13
FIXED	8.x-2.41 · 3.3.13 (needs Drupal 10.3 / 11)
CREDIT	Dan Puccetti · Marcus Johansson · Robert Snyder
CVSS / CWE	Not published

ATTACK CHAIN



01 HOW IT HAPPENED

-  **Access bypass.** Drupal's advisory names no specific routes or fields, only that certain ones lacked proper protection.
-  **Money on the line.** The 'may financially impact the vendor' wording suggests order, price or payment-state tampering, but that is our inference, not confirmed.
-  **Exploited before most patched.** Drupal marked it E:Exploit. No actors, scale or indicators were disclosed.

02 HOW YOU'D KNOW YOU WERE HIT

-  **Order inconsistencies:** totals that don't match line items, adjustments or promotions you didn't create, state changes without payment.
-  **Anonymous or low-privilege requests** to commerce routes that normally need checkout or admin context.
-  **Payment reconciliation gaps** between the gateway's records and Drupal's orders.
-  **Note:** the routes to watch are editorial suggestions, not vendor-confirmed affected endpoints.

03 HOW TO REMEDIATE

-  **Upgrade Commerce Core** to 3.3.13 or 8.x-2.41. Release 3.3.13 also closes SA-CONTRIB-2026-255 to 259.
-  **Run DB updates and clear caches** after upgrading, then re-test checkout end-to-end.
-  **Audit orders** since the module was last updated, focusing on unpaid-but-completed and repriced orders.
-  **Re-check custom routes** and permissions in your own commerce extensions.

04 DEFENDER NOTES

-  **Mind the version wording.** The Hacker News says "through 2.41 / 3.3.13", but Drupal says *below*. Those are the fixed versions.
-  **Same article, different story.** PHP2Shell (CVE-2026-109618/-109619) is unrelated to this advisory.

THE TAKEAWAY

Exploited before most stores patched, with no published indicators. Your order history is the evidence, so patch first and then reconcile.

● ● ● drupal-commerce.sh · check, patch, verify

```
composer show drupal/commerce | grep -E '^versions'
drush pm:list --filter=commerce --status=enabled

# 3.x branch
composer require 'drupal/commerce:^3.3.13' -W
# 8.x-2.x branch
composer require 'drupal/commerce:^2.41' -W

drush updatedb -y && drush cache:rebuild
drush sql:query "SELECT order_id,state,total_price__number,changed FROM commerce_order ORDER BY changed
DESC LIMIT 50"
```

ORDER AUDIT · QUICK WINS

- Completed orders with no captured payment
- Totals that changed after placement
- Orders tied to anonymous or new accounts
- Refunds and edits outside staff hours

DETECTION LAB & TRAINING

Turn today's news
into practice

A 45-minute blue-team workshop built on this issue, three starter hunts, and the response checklist we use for every story. Hunts are starting points. Tune them to your schema before you trust them.

 45-MINUTE BLUE-TEAM WORKSHOP**0-10**
MIN**Supply chain**

List every third-party script on a site; record owner, purpose, SRI status and CSP coverage. Mark which pages handle sessions or money.

10-20
MIN**DevSecOps**

Check GitLab *and* Ruby versions; review sign-up policy, recent CI-lint calls and worker crashes in the past 30 days.

20-30
MIN**Edge & remote access**

Run the ASA exposure commands; inventory TeamViewer versions including portable copies; review tech-workstation privileges.

30-40
MIN**Patch triage**

Match assets to the threat board on page 02; assign owners and dates; document mitigations where patching must wait.

40-45
MIN**Tabletop**

'A vendor script on our checkout page changed at 17:10.' Walk identify → preserve → contain → eradicate → recover → communicate.

 INCIDENT RESPONSE CHECKLIST

- 01** Record time, affected systems, exposure and known facts.
- 02** Preserve logs, crashinfo, memory and disk images before changes.
- 03** Isolate or restrict access without destroying evidence.
- 04** Revoke sessions; rotate credentials, API keys and signing material.
- 05** Apply tested vendor fixes or rebuild from known-good media.
- 06** Validate integrity; watch for recurrence and egress.
- 07** Notify stakeholders, customers and regulators as required.
- 08** Write the post-incident report; update detections and playbooks.

 STARTER HUNTS CSP violations from new origins

```
-- any CSP report source not seen in the prior 30 days
SELECT blocked_uri, count(*) FROM csp_reports
WHERE ts > now() - interval '24 hours'
  AND blocked_uri NOT IN (SELECT DISTINCT blocked_uri FROM csp_reports
    WHERE ts < now() - interval '24 hours')
GROUP BY 1 ORDER BY 2 DESC;
```

 Order totals vs. line items (Drupal Commerce)

```
-- orders whose total drifts from their items; then review adjustments
SELECT o.order_id, o.state, o.total_price__number AS total,
  SUM(i.total_price__number) AS items, o.changed
FROM commerce_order o JOIN commerce_order_item i ON i.order_id =
  o.order_id
GROUP BY o.order_id
HAVING ABS(o.total_price__number - SUM(i.total_price__number)) > 0.01
ORDER BY o.changed DESC LIMIT 100;
```

 Remote-support child processes (Sysmon EID 1)

```
// KQL · suspicious children of TeamViewer
DeviceProcessEvents
| where InitiatingProcessFileName =~ "TeamViewer.exe"
| where FileName in~
  ("cmd.exe", "powershell.exe", "rundll32.exe", "mshta.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine
```

 New accounts hitting CI lint (GitLab)

```
# users created <72h ago calling ci/lint
jq -r 'select(.path|test("ci/lint")) |
[.time, .username, .remote_ip] | @tsv' \
  /var/log/gitlab/gitlab-rails/production_json.log | sort | uniq -c
```

 GLOSSARY

- RUM** Real-user monitoring: a script that measures page performance in visitors' browsers.
- SRI** Subresource Integrity: a hash that makes the browser refuse a changed script.
- EIP-7702** Ethereum upgrade letting an account delegate its code to a contract (tx type 0x04).
- Onigmo** Regular-expression engine bundled in Ruby.
- KEV** CISA's Known Exploited Vulnerabilities catalog, with federal deadlines.

 FIVE HABITS FROM THIS ISSUE

- Pin or self-host every third-party script on money pages
- Patch the runtime, not just the app
- Gate open registration on internet-facing dev tools
- Run support consoles with least privilege
- Keep signing keys and egress logs off the box you're defending

SOURCES & STANDARDS

How we checked this issue

Each story was cross-checked against the vendor's own advisory or the affected organisation's statement first, then independent analysts, then press. Where outlets disagree, we say so.

PRIMARY & SECONDARY SOURCES

Lead · Binance

- TRM Labs: North Korea steals \$6.36B from Binance (trmlabs.com/resources/blog)
- CNBC, Oct 30: Billions in crypto frozen in Binance hack
- Euronews / France 24, Oct 30: Binance confirms major hack, \$2.5bn+ frozen
- SecurityWeek: \$6 Billion Binance hack bears hallmarks of TraderTraitor
- FBI IC3 PSA250226 (Feb 2025): TraderTraitor and the Bybit theft

GitLab / Ruby

- Alpine Linux: GitLab security incident CVE-2026-97229 (alpinelinux.org/posts)
- GitLab patch releases 19.4.2 and 19.5.1 (docs.gitlab.com/releases/patches)
- The Hacker News: Ruby fixes three regex engine bugs
- oss-security, 2026-10-23/24
- SecurityWeek: Max-severity GitLab vulnerability exploited against Alpine

TeamViewer

- TeamViewer Trust Center bulletin TV-2026-1011
- CVE record CVE-2026-111585 (OpenCVE)
- Canadian Centre for Cyber Security AV26-1093
- SecurityWeek: TeamViewer flaw could let malicious hosts take over technicians

Polymarket

- SecurityWeek: \$2 Million drained from Polymarket traders
- GoPlus via KuCoin News: hack linked to DebugBear script
- TheCyberSecGuru: Polymarket front-end supply-chain attack
- Zant: When analytics scripts become an attack
- cside (context, June 2026 incident)

Cisco ASA / FTD

- Cisco advisory cisco-sa-asaftd-tunnel-dos-s6mgkb75
- The Hacker News: CISA adds GitLab RCE and Cisco firewall flaws to KEV
- SecurityOnline: Cisco Secure Firewall vulnerability exploited

Drupal Commerce

- Drupal.org SA-CONTRIB-2026-254
- Drupal Commerce 3.3.13 release notes
- The Hacker News: Hackers actively exploit highly critical Drupal Commerce flaw

FACT-CHECK LEDGER

CVE IDs verified

All four CVE IDs (97229, 76418, 111585, 118539) match vendor advisories and CVE records. Six-digit CVE sequence numbers are valid.

Polymarket loss

Headlines say "\$2M+". On-chain analysis puts it at ~\$2.6–2.71M. We print the range.

Binance total

\$6.36B (TRM) is funds stolen at time of theft, not 'affected'. Frozen funds are not recovered funds.

Cisco severity

DoS with device reload. Not remote code execution.

Alpine outcome

Attempts failed and no code execution was evidenced, though Alpine can't fully exclude it. Releases verified clean.

Drupal versions

Affected means *below* 2.41 / 3.3.13. Some coverage says "through", which is wrong.

KEV due date

Nov 1 comes from The Hacker News; CISA's catalog page couldn't be loaded for confirmation.

WHAT TO WATCH NEXT

Binance root cause

Whether the exchange confirms the engineer-laptop entry point and how the signer was reached.

CVE-2026-110264

The second CVSS 10.0 Onigmo path reaches back to GitLab 7.0, so old instances are exposed.

Laundering routes

TRM expects bridges and OTC brokers next. Watch for issuer and exchange freezes.

KEV confirmation

Check CISA's catalog for the Nov 1 due date and the ransomware-use field.

DebugBear post-mortem

How the vendor's CDN was breached, and whether other customers loaded the drainer.

Drupal disclosure

Affected routes and the fix diff, which would let teams write precise detections.

EDITORIAL STANDARDS

Diagrams in this issue are schematic illustrations of reported attack paths. They are not vendor screenshots, and their routes or code are not indicators of compromise. Commands and hunts are defensive starting points; test them in your environment. Attribution to TraderTraitor is an intelligence assessment by private firms, not a court finding. Loss figures are estimates and will change as recovery continues. Cited reporting belongs to its respective publishers; MAG212 CYBER paraphrases and links rather than reproducing it.