It's Probably Nothing
by Sierra Echo Charlie

EDITION 18 / 2 NOVEMBER 2026

Six billion out the door at Binance

A record crypto heist, plus confirmed exploitation of GitLab's regex RCE and the full Ivanti chain.

4 stories / Listen online - 5:21

THE TAKEAWAY

Four stories this edition, and the first sets a record nobody wanted: Binance has confirmed roughly US$6.3 billion in unauthorised withdrawals, the largest crypto theft on record. Elsewhere CISA has been confirming that attackers are already using bugs patched weeks ago, and a page-speed script turns out to have had rather more authority than any page-speed script should.

01 / THE BRIEF

Binance confirms a record US$6.3 billion in unauthorised withdrawals

Binance's own incident notice, published 29 October, estimates the impact at around US$6.3 billion. Its initial read is that a compromised DevOps engineer's laptop gave access to a service container used to submit the withdrawals, and it reports no evidence that wallet private keys leaked. About US$3 billion has been frozen on-chain with blockchain partners; withdrawals were suspended while deposits kept running. Binance says the SAFU fund and company money will cover all losses, law enforcement is engaged, and a technical post-mortem plus an updated Proof of Reserves will follow remediation.

The Guardian reports experts identifying North Korea as the likely culprit - worth holding lightly for now, since the firmer TraderTraitor naming circulating in secondary coverage hasn't been verified against TRM or Chainalysis directly. And a laptop-to-container path to six billion dollars is a fairly brutal case study in workstation security.

QUALIFICATIONS

North Korea attribution is expert assessment reported by the Guardian, not confirmed; the TraderTraitor naming remains unverified.

SOURCES

Security Incident Update (2026-10-30) - Primary source

North Korea is likely culprit behind $6.3bn crypto hack, 'largest heist in history' - Reporting / context

Binance Hit by $6.3 Billion Crypto Theft Linked to North Korea's TraderTraitor - Reporting / context

02 / THE BRIEF

GitLab's CVSS 10.0 regex RCE is now confirmed exploited

CISA added CVE-2026-97229 to the known-exploited catalogue on 29 October: an unauthenticated integer-overflow RCE in GitLab CE/EE's CI/CD regular-expression compiler, CVSS 10.0. The fix shipped back on 12 October in 19.4.2, 19.3.5 and 19.2.8, and GitLab.com was patched before publication - so the news isn't the bug, it's that someone's using it. The federal due date was 1 November, with forensic triage required. This is a different CVE from the GitLab regexp bug covered here earlier, CVE-2026-110264, in case of déjà vu.

CISA's notes warn that other products embedding the same Ruby/Onigmo regexp code may be affected, so this could travel beyond GitLab. GitLab has released six detections for self-managed instances, and the upgrade runs database migrations - single-node installs will see downtime, so plan for it.

WORTH ASKING

Self-managed GitLab older than 19.2.8, 19.3.5 or 19.4.2 is overdue, and given the triage requirement, patched boxes warrant a pass with the detections too.

QUALIFICATIONS

Exploitation is confirmed by CISA's listing; no attack detail, actor or victims are public.

SOURCES

CISA Adds Two Known Exploited Vulnerabilities to Catalog - Primary source

Known Exploited Vulnerabilities Catalog (CSV) - Primary source

GitLab Critical Patch Release: 19.4.2, 19.3.5, 19.2.8 - Primary source

03 / THE BRIEF

CISA completes the Ivanti chain: three CVEs, bypass to root

The Ivanti Connect Secure chain covered here in mid-October - UTA0576 reaching root on a fully patched box, with the privilege-escalation link then unfixed - has grown. On 30 October CISA added that escalation, CVE-2026-111357, to KEV with a 2 November due date and forensic triage, alongside a newly catalogued third flaw: CVE-2026-118527, which lets a remote authenticated attacker upload attacker-controlled files to a known location, due 13 November. CISA's entries formally document the three CVEs chaining from authentication bypass to root.

QUALIFICATIONS

Fix availability for the privilege escalation is unverified - Ivanti's advisory page failed to load.

SOURCES

CISA Adds Two Known Exploited Vulnerabilities to Catalog - Primary source

Known Exploited Vulnerabilities Catalog (CSV) - Primary source

Ivanti Connect Secure zero-day chain (prior story) - Reporting / context

04 / THE BRIEF

A hijacked page-speed script drained Polymarket traders' wallets

On 29 October, attackers compromised DebugBear's DNS at its domain registrar and swapped the real-user-monitoring script Polymarket embedded on its pages for a wallet drainer. No passwords or seed phrases needed: the script reused logged-in sessions, trading API keys stored in the browser, and Polymarket's own transaction signer and relayer to sell or transfer positions. Roughly US$2.7 million left about 730 wallets in under an hour before Polymarket pulled the script, went cancel-only and paused the relayer. It says everyone will be made whole - US$3.9 million in total, including about US$1.2 million for roughly 5,500 wallets caught by the pause - and has referred the matter to UK authorities.

The awkward part for everyone else: a page-speed snippet effectively held signing authority over user funds. CSP didn't help because the script loaded from an approved host; Subresource Integrity would have rejected the swap. DebugBear says it found no breach of its own systems and believes one customer was targeted - that's its early assessment - and has told RUM customers to remove the embed.

WORTH ASKING

If your site embeds DebugBear's RUM script, that removal advice applies to you right now.

QUALIFICATIONS

Wallet counts differ between sources: 726 per Polymarket's refund figures, 737 per Bitquery via Reflectiz. DebugBear's 'no breach of our systems' is its own early claim.

SOURCES

Polymarket status: exchange in cancel-only mode, relayer paused - Primary source

Hackers Steal About $2.7 Million From Polymarket Traders via Hijacked DebugBear Script - Reporting / context

Polymarket Hack: How a Hijacked DebugBear Script Drained $2.7M - Reporting / context

Compromised DebugBear Script Drains Polymarket Traders' Wallets - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.