It's Probably Nothing
by Sierra Echo Charlie

EDITION 33 / 23 NOVEMBER 2026

AI prompt canaries sing, Expressway hits KEV

Plus two NZ data incidents, an Australian broker breach and an unconfirmed FBI database hack.

5 stories / Listen online - 4:07

THE TAKEAWAY

The best read of the past few days is a research project that seeded about two million prompts with tripwires and watched who tripped them. After that, a Cisco edge bug has gone from quiet to exploited. There's also a cluster of breach disclosures closer to home.

01 / THE BRIEF

Dragos laced two million prompts with canaries, and the AI supply chain leaked

Dragos published this on 19 November. Between July and November it sent roughly two million prompts stuffed with unique URLs and canary credentials to AI services, then watched for anyone using them. It says data from at least three AI hosting providers was exposed to attackers, the earliest from mid-July. None of the three knew until Dragos told them. In the largest breach, every request sent during several late-October windows was stolen, including requests the provider rejected before a model even ran. In the other two, some stolen requests were marked Zero Data Retention.

The stolen canary AWS keys weren't just collected. Dragos says some were tested within hours and used in tens of thousands of API calls. These included S3, Secrets Manager and Parameter Store discovery, plus attempts to enable Bedrock, mint Bedrock API keys and add IAM users for persistence. One attacker brought in the ARTEX AI pentest framework on 1 November, and Dragos suggests watching for the user agents artex-agent and artex-judge-r121.

The non-breach findings are arguably more awkward. Dragos says marketplace resellers were viewing and keeping prompts through ordinary request logging. It also says an unnamed Chinese AI lab fetched the secret URLs from more than half the prompts sent to its models. That included about two-thirds of the ZDR or no-data-collection requests, some routed through US resellers. Dragos's point is that a privacy flag only binds the first hop. ZDR turns out to be a request, not a guarantee.

On 22 November, OpenRouter said there was no breach of OpenRouter itself. It has off-boarded three providers, pulled 125 endpoints from ZDR eligibility and notified potentially affected customers. Neither Dragos nor OpenRouter has named the providers, or said whether the two groups of three are the same. Separately, The Hacker News reports two provider disclosures. Together AI said an unauthorised party downloaded stored customer prompt samples from June-July after an AI coding agent committed a credential to a public GitHub repo. Phala said an attacker controlled an inference server and advised treating requests from 21 October to 8 November as exposed.

WORTH ASKING

If your agents carry real credentials in context and route through a marketplace, it's worth knowing exactly which upstream provider handles them. Dragos recommends going direct or self-hosting, filtering secrets out of prompts and seeding your own canaries.

SOURCES

Three breaches, endless leaks: Your AI supply chain needs canaries - Primary source

Data Processing Incidents on Inference Providers - Primary source

OpenRouter Drops 3 Providers After Researchers Catch Months of Prompt Theft at AI Hosting Firms - Reporting / context

AI Canary Study Finds Evidence of Three Provider Breaches and Prompt Theft - Reporting / context

02 / THE BRIEF

Clustered Cisco Expressway root bug is now exploited and on KEV

CISA added CVE-2026-76466 to KEV on 20 November. Cisco fixed it on 21 October and rated it 9.8. It gives an unauthenticated attacker with network access to the database service root command execution on Expressway-C and Expressway-E. The cause is that persistent cookies and client certificates aren't validated when TLS Verify Mode is enabled for clustering. Only clustered deployments are affected. X15.5.3 and earlier are fixed in X15.5.20, X14 and older need migrating, and there are no workarounds.

Cisco's advisory still says it isn't aware of malicious use. SecurityWeek reports it hadn't been revised as of 19 November, by which point a public proof of concept was out. F6 described the first case on 18 November, shortly after the public exploit appeared. Attackers took root on two internet-facing X15.5.3 boxes at a Russian organisation, then reached two more cluster nodes on the internal network. From there they staged custom Python scripts for scanning, SMB discovery, SQL Server and WinRM work, and trawling GitLab for credentials. F6 says comments in the code suggested an AI assistant helped write them. F6 didn't name the victim or attribute the activity.

WORTH ASKING

For clustered Expressway that can't be upgraded yet, F6 suggests restricting TCP 4371-4372 to trusted cluster-node addresses. It also publishes host-log and file-path indicators for checking whether you've already been hit.

SOURCES

CISA Adds Four Known Exploited Vulnerabilities to Catalog - Primary source

Cisco Expressway Series Remote Code Execution Vulnerability - Primary source

F6 □□□□□□□□□□□□□ □□□□□□ □□□□□□ □□□□□□□□□□□□ □□□□□□□□□□□ □□□□□□□□□□ CVE-2026-76466 □ Cisco Expressway - Primary source

Hackers Exploit Cisco Expressway Vulnerability Soon After PoC Release - Reporting / context

CISA Flags Exploited SAP NetWeaver JNDI Flaw Alongside Three Other Vulnerabilities - Reporting / context

03 / THE BRIEF

NZDF and Forest & Bird both report data accessed

Two separate local incidents surfaced on 20 November, both via RNZ quoting the organisations. NZDF says its website provider told it that morning of unauthorised access to its website systems. It pulled the affected sites and started a forensic investigation. Preliminary inquiries indicate the Force4Families Defence Discounts database was accessed, which holds registered users' names and email addresses. Affected people have been contacted, the Privacy Commissioner has been informed, and the full extent is still being worked out.

Forest & Bird says it was alerted on the evening of 18 November. A forensic search of its website found hidden malicious files reading data, which have now been removed. Mostly names, phone numbers and emails were accessed, but a small subset may have lost payment card details, dates of birth and addresses. The number affected isn't clear, and Police, NCSC and the Privacy Commissioner have been notified. One security expert told RNZ the two incidents are likely unrelated, and there's no attribution for either.

SOURCES

New Zealand Defence Force confirms database compromised, websites removed from service - Reporting / context

Forest & Bird supporters' details stolen by hackers - Reporting / context

Forest & Bird, NZDF cyber attacks likely unrelated, expert says - Reporting / context

Cyber attack hits NZ Defence Force, as personal details of users potentially exposed - Reporting / context

04 / THE BRIEF

Bell Financial says some client data was likely accessed

Across the Tasman, ASX-listed broker Bell Financial Group told the market on 20 November about unauthorised access to a limited number of IT systems. It says the access has been contained, but it believes some clients' data was accessed. Bell says client assets are safe and it's operating as usual. It has notified the ACSC and AFP and engaged with the OAIC. Bell Direct says clients who aren't contacted can assume they weren't affected, and warns of scams and phishing. There's no word yet on data types, numbers or how the attackers got in. Brokerage client lists are prime material for targeted investment scams, so that warning is doing real work.

SOURCES

Bell Financial Group ASX release: Data security incident - Primary source

Important: data security incident | Bell Direct - Primary source

05 / THE BRIEF

FBI reportedly investigating apparent NCIC hack

CNN reported, and AP confirmed through an anonymous source, that the FBI is investigating an apparent hack of the National Crime Information Center. That's the database local, state and federal agencies use for fugitives, missing persons, criminal history and stolen property. The FBI declined to comment and the scope isn't clear. AP saw no immediate sign of a link to recent US outages. For now it's thinly sourced but worth watching.

SOURCES

FBI Investigating Apparent Hack of Its Key National Criminal Justice Database, AP Source Says - Reporting / context

FBI National Crime Information Center Reportedly Breached - 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.