INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-20 06:04 UTC

Lumma Stealer Supply Chain Pivot: Context.ai Compromise Leads to Vercel Infrastructure Access

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0095
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Vercel (infrastructure, customer environment variables), Context.ai (Google Workspace credentials), Next.js, Turbopack, Supabase, Datadog, Authkit
Published	2026-04-19T23:35:00
Discovery Source	Rss

Executive Summary

In February 2026, a Lumma Stealer infection on a Context.ai employee's personal device enabled attackers to harvest Google Workspace credentials and OAuth tokens, which were then used to access Vercel's internal systems and exfiltrate a subset of customer environment variables. ShinyHunters has claimed responsibility and is offering the stolen data for $2 million, though attribution remains medium-confidence based on self-claim only. Organizations using Vercel, particularly those storing sensitive configuration values in environment variables, should audit their Vercel project settings, rotate any potentially exposed secrets, and review third-party SaaS access controls immediately.

Technical Analysis

Attack chain: Lumma Stealer infostealer infected an unmanaged personal device belonging to a Context.ai employee (initial access likely via T1566 phishing or T1566.003 spearphishing). The stealer harvested Google Workspace session tokens and plaintext credentials (CWE-522, CWE-312; MITRE T1539, T1552.001). Attackers reused those OAuth tokens to authenticate into Vercel's internal systems (CWE-287, CWE-565; MITRE T1528, T1550.001, T1078.004), bypassing MFA via token replay (OAuth tokens do not inherently require re-authentication on use) rather than credential stuffing, though the specific mechanism has not been disclosed by Vercel. Lateral movement occurred across Vercel's cloud infrastructure (T1530), accessing a subset of customer non-sensitive environment variables. The breach is classified as a trusted-relationship / supply-chain pivot (T1195.002, T1199). No CVE has been assigned to the breach event itself. Separately, five

Vercel/Next.js platform CVEs exist from the same period: CVE-2025-59471 and CVE-2025-59472 (summarized in Vercel changelog), CVE-2025-55182, CVE-2025-55183, and CVE-2025-55184 (Vercel security bulletins); these are distinct from the breach and affect Next.js and Vercel platform components including Turbopack. Affected integrations include Next.js, Turbopack, Supabase, Datadog, and Authkit configurations stored as environment variables. Source quality is T3/secondary (0.64); Vercel's official changelog should be treated as authoritative for customer impact scope. ShinyHunters attribution is medium-confidence, actor self-claim only, not independently corroborated forensically as of analysis date.

Action Checklist

1. Containment: Log into your Vercel dashboard immediately and review all project environment variables across every team. Identify secrets, API keys, database connection strings, and OAuth credentials. Rotate all exposed values immediately, prioritizing credentials that grant access to downstream systems (Supabase, Datadog, Authkit, payment processors). Do not wait for individual notification from Vercel.
2. Detection: Review Vercel audit logs for anomalous access events, particularly OAuth-based authentication from unfamiliar IP ranges or unusual geographic locations in February-March 2026. Query your IdP (Google Workspace, Okta, etc.) for OAuth token issuance events tied to Vercel. If you use Datadog, check for unexpected API key usage originating outside your normal infrastructure. SIEM: correlate T1528 (steal application access token) and T1550.001 (application access token abuse) indicators against your cloud access logs.
3. Eradication: Revoke and regenerate all Vercel API tokens, team tokens, and any OAuth application credentials connected to your Vercel projects. If any rotated secrets were shared with Supabase, Datadog, Authkit, or other integrated services, rotate those independently as well. Separately, assess and patch the five discrete Vercel/Next.js CVEs (CVE-2025-59471, CVE-2025-59472, CVE-2025-55182, CVE-2025-55183, CVE-2025-55184) per their respective Vercel changelog and security bulletin guidance.
4. Recovery: After rotation, monitor all downstream services for anomalous activity for a minimum of 30 days. Verify that no new OAuth grants were issued to unknown applications. Confirm Vercel project environment variables reflect only current, intentionally stored values. Enable Vercel audit log alerting if not already active. Validate that no build pipeline secrets were cached in CI/CD systems using the compromised values.
5. Post-Incident: This breach exposes three control gaps: (1) unmanaged personal devices with access to corporate SaaS credentials (gap: no MDM or BYOD policy enforcing EDR on personal devices used for work); (2) OAuth token persistence without session binding or anomaly detection; (3) sensitive secrets stored in cloud platform environment variables without secrets-management tooling (e.g., HashiCorp Vault, AWS Secrets Manager). Implement endpoint detection on any device authenticating to corporate SaaS. Enforce short-lived OAuth tokens with binding to device posture. Migrate sensitive secrets out of Vercel environment variables into a dedicated secrets manager.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to legal counsel and initiate breach notification assessment immediately if any rotated Vercel environment variables contained credentials granting access to databases, storage, or services holding PII, PHI, or payment card data — the ShinyHunters $2M listing and confirmed exfiltration of customer environment variables likely triggers GDPR Article 33 (72-hour notification), US state breach notification statutes, or PCI DSS Incident Response requirements depending on data classification of exposed downstream service credentials.
Recovery Notes	Monitor all downstream services integrated via the rotated credentials — specifically Supabase, Datadog, and Authkit — for anomalous API activity, unexpected data exports, or new service account creation for a minimum of 30 days post-rotation, as Lumma Stealer may have harvested credentials with longer-lived downstream sessions not terminated by Vercel token rotation alone. Verify Vercel build cache and deployment logs from February–March 2026 do not contain any residual plaintext secret values from the compromised environment variables, as build output caching in Vercel's infrastructure may persist independently of environment variable rotation. Confirm with each affected downstream vendor (Supabase, Datadog, Authkit) that no new administrative accounts, webhook endpoints, or data export jobs were created during the breach window using the harvested credentials.
Forensic Artifacts	Google Workspace Admin Token Report (Admin Console → Reports → Token): OAuth token issuance and access events for the Vercel OAuth application scoped to February 1 – March 15 2026 — will show the exact timestamp Lumma-harvested Google credentials were replayed to authorize Vercel OAuth access and from which IP/device fingerprint. | Vercel Audit Log (`/v2/teams/{teamId}/audit-log` API or dashboard Settings → Audit Log): `project.env.read` and `project.env.update` event records showing which environment variable namespaces were accessed by the attacker's OAuth session — directly maps the exfiltration scope to specific projects and secret names. | Datadog Audit Trail (`/api/v2/audit`): API authentication events from IPs outside your known infrastructure baseline during the breach window — Lumma-harvested Datadog API keys would appear as legitimate authenticated requests from attacker-controlled hosts, distinguishable by IP geolocation and user-agent anomalies. | Supabase project audit logs and service role key last-used timestamps: if the Supabase service role key was stored in Vercel environment variables, the Supabase dashboard (Project Settings → API) will show last-used timestamps — any access from non-CI/CD IPs during February–March 2026 confirms active use of the harvested key. | CI/CD pipeline execution logs (GitHub Actions, GitLab CI, or equivalent) for February–March 2026 build runs: search for any unexpected workflow triggers, artifact uploads, or environment variable echoing in build output that could indicate an attacker using harvested Vercel API tokens to inject malicious build steps or exfiltrate secrets via build log output.

Per-Action IR Details

Containment — Log into your Vercel dashboard immediately and audit all project environment variables across every team and project. Identify any secrets, API keys, database connection strings, or OAuth client credentials stored there. Rotate all exposed values, prioritizing credentials that grant access to downstream systems (Supabase, Datadog, Authkit, payment processors). Do not wait for Vercel to notify you individually.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (choosing a containment strategy appropriate to the incident type and system criticality)

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Use the Vercel CLI (`vercel env ls --all`) to enumerate environment variables across all projects programmatically without clicking through each dashboard project manually. Pipe output to a file for evidence capture before rotation: `vercel env ls --all > vercel_env_audit_$(date +%Y%m%d).txt`. For downstream Supabase secrets,

use `supabase secrets list` via Supabase CLI to confirm which keys are live. For Datadog, pull active API keys via `curl -X GET 'https://api.datadoghq.com/api/v1/api_key' -H 'DD-API-KEY: ' -H 'DD-APPLICATION-KEY: '` before revoking to document scope.

Evidence: BEFORE rotating any credentials: export the full Vercel project environment variable list via dashboard or CLI and preserve it as a timestamped artifact — this documents the exact secrets potentially exfiltrated and their downstream service scope. Capture Vercel audit log entries (Settings → Audit Log) for the February–March 2026 window showing which environment variable namespaces were accessed and by which authenticated identity. If Datadog is integrated, retrieve the Datadog audit trail for API key usage events during this window (`/api/v2/audit`) before key rotation invalidates the correlation. Preserve OAuth grant records from Google Workspace Admin Console (Admin → Reports → Token) showing which third-party apps (including Vercel OAuth app) held active tokens during the breach window.

Detection — Review Vercel audit logs for anomalous access events, particularly OAuth-based authentication from unfamiliar IP ranges or unusual geographic locations in February–March 2026. Query your IdP (Google Workspace, Okta, etc.) for OAuth token issuance events tied to Vercel. If you use Datadog, check for unexpected API key usage originating outside your normal infrastructure. SIEM: correlate T1528 (steal application access token) and T1550.001 (application access token abuse) indicators against your cloud access logs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (using log analysis and indicator correlation to determine the scope and nature of the incident)

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Google Workspace Admin SDK Reports API to pull OAuth token events for the Vercel OAuth application specifically: `gam report token start 2026-02-01 end 2026-03-15 | grep -i vercel` (using GAM, a free Google Workspace admin tool). For IP geolocation anomaly detection without SIEM, export Vercel audit logs as CSV and run a Python one-liner to flag non-baseline countries: `python3 -c "import csv,sys; [print(r) for r in csv.DictReader(sys.stdin) if r.get('country') not in ['US','CA','GB']]" < vercel_audit.csv`. Apply the public Sigma rule for T1528 (steal application access token) against exported Google Workspace logs using `sigma-cli` against JSON log exports if no SIEM is available.

Evidence: Google Workspace Admin Console → Reports → Token: filter for the Vercel OAuth application, export all token issuance and access events for February 1 – March 15 2026, noting any token grants from IPs outside your organization's known CIDR ranges. Vercel Audit Log (Settings → Audit Log or `/v2/teams/{teamId}/audit-log` API): extract all events of type `project.env.read` or `project.env.update` correlated to OAuth-authenticated sessions. Datadog Audit Trail (`/api/v2/audit`): query for API key authentication events from IPs not in your CI/CD or infrastructure baseline — Lumma-harvested Datadog keys would appear as legitimate API calls from attacker-controlled IPs. Google Workspace login audit (`Reports → Login`): look for the Context.ai employee's Google account accessing Vercel OAuth scopes from an unfamiliar device fingerprint or IP, consistent with Lumma Stealer credential replay.

Eradication — Revoke and regenerate all Vercel API tokens, team tokens, and any OAuth application credentials connected to your Vercel projects. If any rotated secrets were shared with Supabase, Datadog, Authkit, or other integrated services, rotate those independently as well. Separately, assess and patch the five discrete Vercel/Next.js CVEs (CVE-2025-59471, CVE-2025-59472, CVE-2025-55182, CVE-2025-55183, CVE-2025-55184) per their respective Vercel changelog and security bulletin guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (eliminating components of the incident including malicious code, unauthorized accounts, and vulnerable configurations)

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without centralized token management tooling: use the Vercel REST API to enumerate and revoke all team tokens programmatically — `curl -X DELETE 'https://api.vercel.com/v3/user/tokens/{tokenId}' -H 'Authorization: Bearer '` — iterating over the full token list retrieved via `GET /v3/user/tokens`. For the five Next.js/Turbopack CVEs, run `npm audit` and `npx next info` to confirm current Next.js version, then upgrade to the patched release specified in the Vercel security changelog. For Supabase secret rotation without a secrets manager, use `supabase secrets set KEY=newvalue` via CLI and immediately redeploy affected functions to pick up new values. Document each rotation with a timestamp and the identity that performed it.

Evidence: Before revoking Vercel OAuth application credentials: capture the full OAuth application authorization list from your Google Workspace Admin Console (Admin → Security → API Controls → App Access Control) documenting which Vercel OAuth app scopes were granted and to which users. Before rotating Supabase service role keys: export current Supabase project API settings and note the `anon` vs `service_role` key fingerprints — Lumma-harvested keys would be the service_role key if it was stored in Vercel environment variables. For the five CVEs (CVE-2025-59471, CVE-2025-59472, CVE-2025-55182, CVE-2025-55183, CVE-2025-55184): capture current Next.js and Turbopack package versions from `package-lock.json` or `yarn.lock` before patching, and preserve any build logs from February 2026 that might indicate exploitation attempts against the vulnerable versions.

Recovery — After rotation, monitor all downstream services for anomalous activity for a minimum of 30 days. Verify that no new OAuth grants were issued to unknown applications. Confirm Vercel project environment variables reflect only current, intentionally stored values. Enable Vercel audit log alerting if not already active. Validate that no build pipeline secrets were cached in CI/CD systems using the compromised values.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (restoring systems to normal operation and verifying that systems are fully functional, while monitoring for recurrence)

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For CI/CD secret cache validation without enterprise tooling: audit GitHub Actions, GitLab CI, or Bitbucket Pipelines environment variable stores manually — check repository Settings → Secrets and Variables for any references to the compromised Vercel, Supabase, Datadog, or Authkit key values (search for the first 8 characters of old key values as a pattern). For ongoing OAuth grant monitoring without a CASB: schedule a weekly cron job calling the Google Workspace Admin SDK `GET /admin/reports/v1/activity/users/all/applications/token` endpoint and diff against a known-good baseline to flag new Vercel OAuth grants. Use `osquery` on developer workstations with the query `SELECT * FROM browser_extensions WHERE identifier LIKE '%vercel%'` to detect any unauthorized Vercel integrations cached locally.

Evidence: After rotation and redeployment: pull a fresh Vercel audit log export and verify that all `project.env.read` events post-rotation are attributed only to known CI/CD service accounts and authorized team members. Query Google Workspace token report for any new Vercel OAuth authorization grants issued after your rotation date — any grant to an unrecognized application ID indicates residual attacker persistence. For Datadog: use `/api/v2/audit?filter[action]=created&filter[resource_type]=api_key` to confirm no new API keys were silently created during the breach window using harvested application keys. Check GitHub Actions or your CI system's workflow run logs for the compromised key patterns appearing in build output (secrets masking bypass artifacts).

Post-Incident — This breach exposes three control gaps: (1) unmanaged personal devices with access to corporate SaaS credentials (gap: no MDM or BYOD policy enforcing EDR on personal devices used for work); (2) OAuth token persistence without session binding or anomaly detection; (3) sensitive secrets stored in cloud platform environment variables without secrets-management tooling (e.g., HashiCorp Vault, AWS Secrets Manager). Implement endpoint detection on any device authenticating to corporate SaaS. Enforce short-lived OAuth tokens with binding to device posture. Migrate sensitive secrets out of Vercel environment variables into a dedicated secrets manager.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (lessons learned, evidence retention, and using incident data to improve controls and prevent recurrence)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-3 (Malicious Code Protection), NIST IA-5 (Authenticator Management), NIST CM-7 (Least Functionality), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without MDM budget: enforce Google Workspace Context-Aware Access (free with Google Workspace Business Standard and above) to require device enrollment or certificate presence before OAuth tokens are issued to Vercel or other SaaS integrations — this directly addresses the Lumma Stealer personal-device vector by blocking unmanaged device OAuth grants. For secrets management without Vault or AWS Secrets Manager: migrate Vercel environment variable secrets to Doppler (free tier available) or use `age`-encrypted secret files stored in version control with key access limited to CI/CD service accounts — eliminates plaintext secrets in Vercel's environment variable store. For OAuth token lifetime reduction: in Google Workspace Admin → Security → API Controls, set OAuth token session length to 1 hour for third-party applications including Vercel, limiting the window a Lumma-harvested token remains valid.

Evidence: For the lessons-learned record: preserve the full incident timeline artifact documenting the Lumma Stealer infection date on the Context.ai employee device, the first anomalous Vercel OAuth access timestamp, and the ShinyHunters claim date — this establishes dwell time for regulatory disclosure calculations. Retain the Google Workspace token audit export showing the OAuth scopes granted to the Vercel application at time of compromise — required to assess data exposure scope under GDPR Article 33 or applicable US state breach notification laws if customer PII was reachable via exposed environment variables. Document the specific Vercel environment variable names (not values) that were exposed — this scopes which downstream vendors (Supabase, Datadog, Authkit) require their own breach notification assessments and serves as evidence of control gap (secrets in platform env vars rather than a dedicated secrets manager).

Detection Guidance

Primary detection surface is OAuth and cloud access logs. Query your IdP audit logs for Vercel OAuth token issuance and token reuse events from February 2026 onward, flagging sessions where token origin IP does not match the authenticating user's historical geographic or network baseline (MITRE T1550.001, T1528). In Vercel audit logs, look for environment variable read/export events outside normal deployment pipelines, specifically any access not tied to a known CI/CD service account. If using Google Workspace, review OAuth application authorization events for Vercel and connected apps; revoke any unrecognized grants. For Lumma Stealer specifically: on endpoints, look for process injection into browsers (targeting Chrome, Edge, Firefox credential stores), LSASS access attempts, and cross-reference indicators against current threat intelligence feeds for Lumma C2 infrastructure. Note: no specific C2 IOCs have been publicly disclosed for this incident. SIEM detection logic should correlate: (1) new OAuth grant to Vercel from an unfamiliar device + (2) environment variable access within the same session window. Behavioral indicator: large-volume environment variable reads in a short timeframe from a single authenticated session.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Not available — no confirmed IOCs extracted from current sources`	Lumma Stealer C2 infrastructure IOCs rotate frequently and were not confirmed in the source data for this incident. Check current threat intelligence feeds (e.g., abuse.ch, ETPRO, vendor TI platforms) for active Lumma Stealer C2 indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1528** — Steal Application Access Token
- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1552.001** — Credentials In Files
- **T1078.004** — Cloud Accounts
- **T1199** — Trusted Relationship
- **T1556.006** — Multi-Factor Authentication
- **T1550.001** — Application Access Token
- **T1530** — Data from Cloud Storage
- **T1195.002** — Compromise Software Supply Chain
- **T1566.003** — Spearphishing via Service
- **T1539** — Steal Web Session Cookie

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity

- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1528	Steal Application Access Token	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1552.001	Credentials In Files	Credential-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1199	Trusted Relationship	Initial-Access

Technique ID	Technique Name	Tactic
T1556.006	Multi-Factor Authentication	Credential-Access
T1550.001	Application Access Token	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1195.002	Compromise Software Supply Chain	Initial-Access
T1566.003	Spearphishing via Service	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/vercel-breach-tied-to-context-ai-...	T3
Summaries of CVE-2025-59471 and CVE-2025-59472 - Vercel	https://vercel.com/changelog/summaries-of-cve-2025-59471-and-cve-20...	T3
Critical Security Vulnerability in Next.js Caused Server Abuse ...	https://github.com/vercel/next.js/discussions/86977	T3
Security Bulletin: CVE-2025-55184 and CVE-2025-55183 - Vercel	https://vercel.com/kb/bulletin/security-bulletin-cve-2025-55184-and...	T3
Summary of CVE-2025-55182 - Vercel	https://vercel.com/changelog/cve-2025-55182	T3

Generated 2026-04-20 06:04 UTC by TJS Security Command Center