INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-20 05:33 UTC

Vercel Breach Traced to Third-Party AI Tool OAuth Compromise: CI/CD Pipeline Credentials at Risk

DATA BREACH | CRITICAL | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0094
Type	Data Breach
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Vercel (cloud development platform, Next.js, Turbopack, serverless/edge infrastructure); Context.ai (third-party AI platform, initial access vector); Google Workspace (OAuth application abuse); downstream Vercel developer customers with exposed environment variables
Published	2026-04-19T13:32:45
Discovery Source	Rss

Executive Summary

Vercel, the cloud development platform powering a significant portion of modern web applications, confirmed unauthorized access to internal systems after a threat actor compromised a Vercel employee's Google Workspace account through a breach at Context.ai, a third-party AI platform connected via OAuth. The attacker accessed unencrypted environment variables containing API keys, NPM tokens, and GitHub tokens belonging to Vercel's developer customer base, creating direct downstream supply chain risk for any organization running production workloads on Vercel. A threat actor claiming ShinyHunters affiliation announced the stolen data for sale and demanded a $2 million ransom (unverified), elevating this from a vendor incident to an active threat requiring immediate credential rotation across affected pipelines. Breach discovery: early April 2026.

Technical Analysis

Attack chain: Threat actor breached Context.ai (third-party AI platform), obtained a valid OAuth token for a Vercel employee's Google Workspace account, and leveraged that token to escalate access into Vercel internal environments. This incident is a vendor breach, not a product vulnerability, so no CVE applies to the breach itself. Relevant CWEs: CWE-287 (improper authentication via OAuth token abuse), CWE-522 (insufficiently protected credentials, unencrypted environment variables), CWE-312 (cleartext storage of sensitive

information), CWE-200 (exposure of sensitive information), CWE-1390 (weak authentication). MITRE techniques: T1199 (Trusted Relationship), T1078.004 (Valid Accounts: Cloud Accounts), T1550.001 (Use Alternate Authentication Material: Application Access Token), T1552.001 (Credentials in Files), T1530 (Data from Cloud Storage), T1195.001 (Supply Chain Compromise: Compromise Software Dependencies and Development Tools), T1657 (Financial Theft, ransom demand). Exposed data includes environment variables stored in Vercel's internal systems: API keys, NPM tokens, and GitHub tokens associated with customer projects. ShinyHunters affiliation is claimed, not independently verified. Patch status: No patch applies to the breach vector itself; remediation is credential rotation and OAuth scope review.

Action Checklist

1. Containment: Immediately audit all OAuth applications connected to employee Google Workspace and corporate identity providers; revoke Context.ai OAuth grants immediately and verify removal within 1 hour via OAuth app audit logs; suspend affected tokens before rotating to prevent parallel session abuse.
2. Detection: Query CI/CD pipeline logs and GitHub audit logs for anomalous API key usage, unexpected NPM publish events, or GitHub token activity originating from unfamiliar IPs or user agents since early April 2026; review Vercel project environment variable access logs for unauthorized reads; check Google Workspace audit logs for OAuth token grants to Context.ai or other AI platforms.
3. Eradication: Rotate all secrets stored as Vercel environment variables: API keys, NPM tokens, GitHub personal access tokens, and any service account credentials; revoke and reissue GitHub fine-grained tokens scoped to Vercel integrations; remove Context.ai OAuth grants from all connected Google Workspace accounts; audit NPM organization for unauthorized package publishes.
4. Recovery: After rotating credentials, redeploy all affected Vercel projects to purge cached environment variables; verify new tokens are functioning in staging before promoting to production; monitor NPM registry and GitHub repositories for unauthorized commits or package versions published during the exposure window; confirm no new OAuth grants were silently re-established.
5. Post-Incident: This attack exposed two control gaps: unencrypted storage of secrets in CI/CD environment variables and insufficient third-party OAuth scope governance. Implement secrets management (HashiCorp Vault, AWS Secrets Manager, or equivalent) to replace plaintext environment variable storage; enforce least-privilege OAuth scopes for all third-party integrations; add third-party AI platforms to your vendor risk assessment process; require periodic OAuth grant reviews as a recurring control.

Detection Guidance

GitHub Audit Log: Filter for events token_type:personal_access_token or oauth_access_token with actor IP addresses not matching known Vercel or employee egress ranges. Flag any repository.create, repository.destroy, or workflow_run events from unexpected actors. NPM: Check organization publish history for packages published outside normal release windows or by unfamiliar tokens; use `npm audit log` or registry webhook alerts. Vercel Dashboard: Review Environment Variables access logs under Project Settings for read events not initiated by known CI/CD service accounts. Google Workspace Admin Console: Audit OAuth app grants under Security > API Controls > App Access Control; look for Context.ai or unknown AI platform grants with broad scopes (drive, gmail, openid). SIEM behavioral indicators: Spike in outbound API calls from CI/CD worker IPs to unfamiliar endpoints; environment variable reads outside deployment pipelines; new OAuth token

grants to third-party apps during off-hours. IOC note: No confirmed IOCs (IPs, domains, hashes) have been publicly released for this incident as of the source data; treat any IOCs circulating on social media as unverified.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`context.ai`	Third-party AI platform identified as initial access vector via OAuth compromise; treat integrations with this service as potentially compromised	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1552.001** — Credentials In Files
- **T1136.003** — Cloud Account
- **T1199** — Trusted Relationship
- **T1657** — Financial Theft
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1078.004** — Cloud Accounts
- **T1552** — Unsecured Credentials
- **T1530** — Data from Cloud Storage
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1550.001** — Application Access Token
- **T1195** — Supply Chain Compromise

NIST-800-53R5

- **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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan

- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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
- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

NIST-CSF-2

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552.001	Credentials In Files	Credential-Access
T1136.003	Cloud Account	Persistence
T1199	Trusted Relationship	Initial-Access
T1657	Financial Theft	Impact
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1552	Unsecured Credentials	Credential-Access
T1530	Data from Cloud Storage	Collection
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion
T1195	Supply Chain Compromise	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/vercel-confirms-brea...	T3
Vercel April 2026 security incident - Hacker News	https://news.ycombinator.com/item?id=47824463	T3
Cloud development platform Vercel was hacked - Facebook	https://www.facebook.com/verge/posts/cloud-development-platform-ver...	T3
Security Bulletin: CVE-2025-55184 and CVE-2025-55183 - Vercel	https://vercel.com/kb/bulletin/security-bulletin-cve-2025-55184-and...	T3
New deployments of vulnerable Next.js applications are ... - Vercel	https://vercel.com/changelog/new-deployments-of-vulnerable-next-js-...	T3

Generated 2026-04-20 05:33 UTC by TJS Security Command Center