INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 06:51 UTC

SaaS Integrator Breach at Anodot Exposes Downstream Customers via Stolen Auth Tokens, ShinyHunters Adds Vimeo to Extortion Queue

DATA BREACH | **HIGH** | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0106
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Anodot (data anomaly detection platform), Vimeo, Rockstar Games, Snowflake (cloud data platform), Google BigQuery
Published	2026-04-28T15:04:22
Discovery Source	Rss

Executive Summary

ShinyHunters compromised Anodot, a third-party SaaS analytics vendor, by stealing authentication tokens that granted direct access to cloud data environments at multiple downstream customers, including Vimeo and Rockstar Games. Vimeo has confirmed exposure of customer email addresses, video metadata, and technical data; no passwords or payment information are confirmed compromised at this time. ShinyHunters has set an April 30 extortion deadline for Vimeo, threatening public release of stolen data if payment is not made, creating immediate reputational and regulatory exposure for all affected organizations.

Technical Analysis

ShinyHunters executed a SaaS supply chain attack against Anodot, a cloud-based data anomaly detection platform with integrations into Snowflake and Google BigQuery environments belonging to its customers. The attack vector was stolen authentication tokens held by Anodot on behalf of its customers (T1528, Steal Application Access Token; T1539, Steal Web Session Cookie), which the actor used to authenticate as a trusted SaaS integrator and access downstream cloud storage buckets (T1530, Data from Cloud Storage; T1078.004, Valid Accounts: Cloud Accounts). Lateral movement from Anodot into multiple customer environments reflects a supply chain compromise pattern in which the compromised intermediary (Anodot) served as an authenticated gateway to downstream targets (T1195.003, Supply Chain Compromise: Compromise Software Dependencies; CWE-441, Unintended Proxy/Intermediary). Data exfiltration followed (T1567.002, Exfiltration to Cloud Storage).

The extortion phase is tracked under T1657. Relevant weaknesses: CWE-287 (Improper Authentication, token-based auth bypass at the integrator layer), CWE-522 (Insufficiently Protected Credentials, inadequate token storage and rotation controls at Anodot), CWE-359 (Exposure of Private Personal Information, downstream PII access at victim organizations). No CVE has been assigned. No vendor patch is applicable; this is a credential hygiene and architectural control failure, not a software vulnerability in the traditional sense. Confirmed affected: Vimeo (email addresses, video metadata, technical data). Snowflake and Google BigQuery instances at additional unnamed customers are reported affected. Anodot has not issued a public technical advisory as of this writing.

Action Checklist

1. Step 1: Containment, Audit all third-party SaaS integrators that hold OAuth tokens, API keys, or service account credentials with access to your Snowflake, Google BigQuery, or other cloud data platforms. Immediately revoke and rotate any tokens issued to Anodot or other integrators you cannot confirm are uncompromised. Suspend Anodot integrations in your environment pending confirmation from Anodot that the breach is contained.
2. Step 2: Detection, Review cloud audit logs in Snowflake (Account Usage > QUERY_HISTORY, LOGIN_HISTORY) and Google BigQuery (Cloud Audit Logs > Data Access logs) for authentication events using service account or OAuth credentials associated with Anodot or any anomalous third-party identity. Look for data read or export operations outside normal business hours or involving bulk row counts inconsistent with normal Anodot query patterns. Check for T1530 indicators: large SELECT operations, COPY INTO external stage commands (Snowflake), or BigQuery export jobs initiated by service accounts.
3. Step 3: Eradication, Revoke all active tokens and service account keys provisioned for Anodot. Issue new credentials following least-privilege principles, scoping access only to the datasets Anodot requires. Enable Snowflake Network Policies and Google BigQuery VPC Service Controls to restrict integrator access to known IP ranges. Confirm with Anodot in writing that compromised credential material has been invalidated on their end.
4. Step 4: Recovery, After re-issuing credentials, validate that only expected integrator identities appear in fresh cloud audit logs. Monitor for any resumed anomalous access patterns for a minimum of 30 days. Confirm data classification for all datasets the integrator had access to, and assess whether exposed data triggers breach notification obligations under applicable regulations.
5. Step 5: Post-Incident, This attack exposed a systemic gap: third-party SaaS integrators often hold standing, broadly scoped credentials to customer cloud environments without adequate monitoring or token rotation policies. Implement a SaaS integrator inventory program. Enforce token expiration and rotation policies (maximum 90-day token lifetime as a baseline). Require integrators to use short-lived credentials or OAuth with PKCE where the platform supports it. Add cloud data platform access to your third-party risk assessment process.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if Snowflake QUERY_HISTORY or BigQuery audit logs confirm bulk data exports from tables containing PII (email addresses, user identifiers, or payment-adjacent fields), as this triggers breach notification obligations under GDPR (72-hour window), CCPA, or applicable state laws — or if any evidence confirms ShinyHunters has already published or sold your organization's data ahead of the April 30 Vimeo extortion deadline.
Recovery Notes	After re-issuing Anodot credentials under least-privilege scope and network restrictions, run a 30-day continuous audit of Snowflake ACCESS_HISTORY and BigQuery Data Access logs comparing the new service account's query patterns against the pre-breach baseline to detect any residual unauthorized identity operating with previously unknown credentials. Simultaneously, complete data classification for all Snowflake databases and BigQuery datasets the Anodot service account could read — the confirmed Vimeo exposure of customer email addresses and video metadata means analogous data fields in your environment must be evaluated for notification obligations before the ShinyHunters April 30 deadline creates reputational pressure. Document all recovery actions with timestamps for potential regulatory submissions.
Forensic Artifacts	Snowflake ACCOUNT_USAGE.QUERY_HISTORY: rows where USER_NAME matches Anodot service account and QUERY_TEXT contains 'COPY INTO @' (external stage exfil), 'CREATE STAGE', or SELECT statements with ROWS_PRODUCED exceeding normal Anodot analytical query volume — primary artifact establishing what ShinyHunters extracted and when. | Snowflake ACCOUNT_USAGE.LOGIN_HISTORY: CLIENT_IP, CLIENT_APPLICATION_ID, and EVENT_TIMESTAMP for all Anodot service account sessions — cross-reference IPs against Anodot's declared infrastructure to identify sessions originating from ShinyHunters-controlled infrastructure after token theft. | GCP Cloud Audit Log entries for BigQuery jobservice.insert with configuration.extract.destinationUris field populated — any extract job pointing to a GCS bucket outside your organization's GCP project indicates active exfiltration using the stolen Anodot OAuth token. | OAuth authorization server logs: token grant and refresh events for the Anodot client_id, specifically any token refresh activity after the date Anodot's breach occurred — an attacker maintaining a stolen refresh token would generate refresh events from anomalous IPs not matching Anodot's production infrastructure. | Snowflake ACCOUNT_USAGE.STAGES and ACCOUNT_USAGE.ACCESS_HISTORY: any EXTERNAL STAGE objects created under Anodot credentials referencing S3, Azure Blob, or GCS URIs not belonging to your organization — these represent exfiltration staging infrastructure that ShinyHunters may have created and left behind for continued data pull operations.

Per-Action IR Details

Step 1: Containment — Audit all third-party SaaS integrators that hold OAuth tokens, API keys, or service account credentials with access to your Snowflake, Google BigQuery, or other cloud data platforms. Immediately revoke and rotate any tokens issued to Anodot or other integrators you cannot confirm are uncompromised. Suspend Anodot integrations in your environment pending confirmation from Anodot that the breach is contained.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected credentials and integrations to prevent continued ShinyHunters access via stolen Anodot OAuth tokens before scope is fully determined.

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without a PAM or secrets management tool: run `SELECT * FROM SNOWFLAKE.ACCOUNT_USAGE.ACCESS_HISTORY WHERE USER_NAME ILIKE '%anodot%' ORDER BY

QUERY_START_TIME DESC;` to identify all active Anodot service accounts. In GCP, run `gcloud iam service-accounts list --filter='displayName:anodot'` and `gcloud iam service-accounts keys list --iam-account=[SA_EMAIL]` to enumerate keys, then disable immediately with `gcloud iam service-accounts disable [SA_EMAIL]`. Maintain a manual spreadsheet mapping each SaaS integrator to its credential type, scope, and last-rotated date as a stopgap inventory.

Evidence: Before revoking, capture a full snapshot of: Snowflake ACCOUNT_USAGE.ACCESS_HISTORY and LOGIN_HISTORY filtered on Anodot service account names and associated OAuth client IDs (preserving CLIENT_IP, QUERY_TEXT, ROWS_PRODUCED columns); GCP Cloud Audit Logs for `google.iam.admin.v1.GetServiceAccountKey` and `google.cloud.bigquery.v2.JobService.InsertJob` events tied to the Anodot service account email; current token metadata from your OAuth authorization server showing issued_at, scope, and last_used timestamps for Anodot client credentials — these timestamps establish the attacker's access window and data volume before ShinyHunters exfiltrated.

Step 2: Detection — Review cloud audit logs in Snowflake (Account Usage > QUERY_HISTORY, LOGIN_HISTORY) and Google BigQuery (Cloud Audit Logs > Data Access logs) for authentication events using service account or OAuth credentials associated with Anodot or any anomalous third-party identity. Look for data read or export operations outside normal business hours or involving bulk row counts inconsistent with normal Anodot query patterns. Check for T1530 indicators: large SELECT operations, COPY INTO external stage commands (Snowflake), or BigQuery export jobs initiated by service accounts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate Snowflake and BigQuery audit telemetry against known ShinyHunters TTPs (T1530 — Data from Cloud Storage Object) to establish breach timeline and data scope.

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

Compensating: Without a SIEM, run this Snowflake SQL directly against ACCOUNT_USAGE (30-day retention): `SELECT USER_NAME, CLIENT_IP, QUERY_TYPE, ROWS_PRODUCED, QUERY_TEXT, START_TIME FROM SNOWFLAKE.ACCOUNT_USAGE.QUERY_HISTORY WHERE USER_NAME ILIKE '%anodot%' AND (QUERY_TYPE='SELECT' AND ROWS_PRODUCED > 10000 OR QUERY_TEXT ILIKE '%COPY INTO%') ORDER BY START_TIME DESC;` For BigQuery, use the GCP Console Log Explorer query: `resource.type="bigquery_resource" AND protoPayload.authenticationInfo.principalEmail:[anodot-service-account-email] AND protoPayload.methodName="jobservice.insert"` and filter for `configuration.extract` job type indicating export operations. Export results to CSV and manually baseline against known Anodot query volumes.

Evidence: Collect before analysis: Snowflake QUERY_HISTORY rows where QUERY_TEXT contains `COPY INTO @` (external stage exfil), `CREATE STAGE`, or bulk SELECT with ROWS_PRODUCED > org-defined threshold — ShinyHunters would have used Anodot's existing query permissions to extract at scale; BigQuery `jobservice.insert` audit log entries with `configuration.extract.destinationUris` pointing to external GCS buckets not owned by your org; Snowflake LOGIN_HISTORY rows showing CLIENT_IP values for Anodot service account logins — cross-reference against Anodot's disclosed incident timeline to identify sessions occurring after the token theft; OAuth token issuance logs from your identity provider showing Anodot client_id grant history, specifically any token refresh activity that would indicate the stolen token was actively rotated by the attacker to maintain persistence.

Step 3: Eradication — Revoke all active tokens and service account keys provisioned for Anodot. Issue new credentials following least-privilege principles, scoping access only to the datasets Anodot requires. Enable Snowflake Network Policies and Google BigQuery VPC Service Controls to restrict integrator access to known IP ranges. Confirm with Anodot in writing that compromised credential material has been invalidated on their end.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the ShinyHunters access vector by invalidating stolen Anodot credential material and re-establishing access boundaries with network-layer controls to prevent re-entry via the same token-theft pathway.

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: In Snowflake, create a Network Policy restricting Anodot's new service account to Anodot's declared static IP range: `CREATE NETWORK POLICY anodot_policy ALLOWED_IP_LIST=('x.x.x.x/24'); ALTER USER anodot_svc_account SET NETWORK_POLICY=anodot_policy;` In GCP, configure a VPC Service Controls perimeter via `gcloud access-context-manager perimeters create` restricting BigQuery API access to Anodot's declared source IPs. Obtain Anodot's written confirmation (email with ticket ID is acceptable) stating the specific token IDs or client credential hashes they have invalidated — this documentation is required for breach notification records under NIST IR-6 (Incident Reporting).

Evidence: Before issuing new credentials, document: the full list of Snowflake ROLES granted to the Anodot service account (run `SHOW GRANTS TO USER anodot_svc_account`) and GCP IAM policy bindings (`gcloud projects get-iam-policy [PROJECT_ID] --flatten='bindings[].members' --filter='bindings.members:[anodot-sa-email]'`) — this establishes the blast radius of what data ShinyHunters could have accessed; any Snowflake EXTERNAL STAGE objects (`SHOW STAGES IN ACCOUNT`) created under Anodot credentials pointing to external S3 or Azure Blob locations, which would represent active exfiltration infrastructure left behind; Anodot's written disclosure including the date/time the breach was detected and the credential identifiers compromised — required to verify their-end invalidation is complete.

Step 4: Recovery — After re-issuing credentials, validate that only expected integrator identities appear in fresh cloud audit logs. Monitor for any resumed anomalous access patterns for a minimum of 30 days. Confirm data classification for all datasets the integrator had access to, and assess whether exposed data triggers breach notification obligations under applicable regulations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore Anodot integration under verified least-privilege credentials, confirm no residual ShinyHunters access paths exist, and complete data classification review to determine GDPR/CCPA/state breach notification obligations for the email address and metadata exposure confirmed at Vimeo.

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST RA-3 (Risk Assessment), NIST SI-2 (Flaw Remediation), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Schedule a daily cron job for 30 days that runs the Snowflake QUERY_HISTORY query from Step 2 and emails results to the IR lead — use `snowsql -q "SELECT ..." | mail -s 'Daily Anodot Access Review' ir-team@yourorg.com` or equivalent. For breach notification scoping, manually cross-reference Snowflake table names accessed (from QUERY_HISTORY.QUERY_TEXT) against your data classification inventory to identify PII fields (email, name, user ID) — if your org lacks a formal classification inventory, treat any table with 'user', 'customer', 'email', or 'account' in the name as potentially notifiable pending review.

Evidence: During the 30-day monitoring window, preserve: daily exports of Snowflake ACCESS_HISTORY and BigQuery audit logs filtered on the new Anodot service account identity to establish a clean baseline; any alert triggers from Snowflake's built-in Alerts (`CREATE ALERT` on ROWS_PRODUCED thresholds) or GCP Cloud Monitoring anomaly detections; written confirmation from your legal or compliance team documenting the breach notification decision and its basis (datasets accessed, PII fields confirmed, regulatory jurisdiction) — this record is required under NIST IR-6 (Incident Reporting) and directly relevant given ShinyHunters' April 30 extortion deadline for Vimeo, which creates a corroborating timeline for your own notification timing.

Step 5: Post-Incident — This attack exposed a systemic gap: third-party SaaS integrators often hold standing, broadly scoped credentials to customer cloud environments without adequate monitoring or token rotation policies. Implement a SaaS integrator inventory program. Enforce token expiration and rotation policies (maximum 90-day token lifetime as a baseline). Require integrators to use short-lived credentials or OAuth with PKCE where the platform supports it. Add cloud data platform access to your third-party risk assessment process.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: document lessons learned specific to SaaS integrator credential hygiene gaps exposed by the ShinyHunters/Anodot attack chain and update third-party risk processes to prevent recurrence via the same token-theft supply chain vector.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SA-9 (External System Services), NIST AC-2 (Account Management), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Build the SaaS integrator inventory as a plain spreadsheet with columns: Integrator Name, Credential Type (OAuth/API Key/Service Account), Credential Scope, Issuing Platform (Snowflake/BigQuery/Other), Issue Date, Last Rotated, Expiry Date, Least-Privilege Confirmed (Y/N), Network Restriction Applied (Y/N). Review and update monthly. For token expiration enforcement in Snowflake, set `ALTER USER anodot_svc_account SET DAYS_TO_EXPIRY=90;`. In GCP, use `gcloud iam service-accounts keys create` with a calendar reminder for 90-day key rotation since GCP does not auto-expire SA keys. Publish a YARA or Sigma rule to detect future Anodot-style token abuse: alert on any Snowflake or BigQuery service account executing COPY INTO or extract jobs where the initiating identity is not on a pre-approved integrator allowlist.

Evidence: Post-incident documentation package should include: the complete timeline of Anodot token issuance through ShinyHunters exfiltration, reconstructed from LOGIN_HISTORY and QUERY_HISTORY timestamps, to support the lessons-learned report required by NIST IR-4 (Incident Handling); a gap analysis comparing your pre-incident third-party risk assessment for Anodot against the MITRE ATT&CK T1530 (Data from Cloud Storage Object) and T1552.001 (Credentials in Files) TTPs demonstrated in this breach; and your updated vendor security questionnaire addendum requiring SaaS integrators to attest to credential storage practices, token rotation policies, and breach notification SLAs — directly informed by the Anodot incident where downstream customers were not promptly notified.

Detection Guidance

Snowflake: Query SNOWFLAKE.ACCOUNT_USAGE.LOGIN_HISTORY and QUERY_HISTORY filtering on USER_NAME values associated with Anodot service accounts. Flag authentication events from unexpected source IP addresses, bulk data reads (row counts significantly above baseline), and COPY INTO EXTERNAL STAGE commands. Google BigQuery: Review Cloud Audit Logs (cloudaudit.googleapis.com/data_access) for bigquery.tables.getData and bigquery.jobs.create events initiated by Anodot-associated service accounts. Flag export jobs (bigquery.jobs.create with jobType=EXPORT) and cross-project data access. Behavioral indicators: authentication from Anodot service accounts during non-business hours, queries spanning datasets not normally accessed by Anodot, and data volumes inconsistent with anomaly detection workloads. MITRE techniques to hunt: T1528 (token theft indicators in identity provider logs), T1530 (cloud storage reads), T1567.002 (exfiltration via cloud storage exports). No public IOCs (IPs, domains, hashes) have been confirmed for this specific campaign as of this writing.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs publicly attributed to this campaign`	No IPs, domains, file hashes, or URLs have been publicly confirmed for this ShinyHunters campaign against Anodot as of the source publication dates. Monitor threat intelligence feeds for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1528** — Steal Application Access Token
- **T1539** — Steal Web Session Cookie
- **T1078.004** — Cloud Accounts
- **T1530** — Data from Cloud Storage
- **T1567.002** — Exfiltration to Cloud Storage
- **T1195.003** — Compromise Hardware Supply Chain
- **T1078** — Valid Accounts
- **T1657** — Financial Theft
- **T1195.001** — Compromise Software Dependencies and Development Tools

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan
- **SI-4** — System Monitoring

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
- **8.2** — Collect Audit Logs

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **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
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1528	Steal Application Access Token	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1078.004	Cloud Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1195.003	Compromise Hardware Supply Chain	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/video-service-vimeo-...	T3
	https://www.bleepingcomputer.com/news/security/french-govt-agency-c...	T3
Anodot third-party security incident - Vimeo	https://vimeo.com/blog/post/anodot-third-party-security-incident	T3

Source	URL	Tier
Video service Vimeo confirms Anodot breach exposed user data	https://www.bleepingcomputer.com/news/security/video-service-vimeo-...	T3
Vimeo faces extortion demands from ShinyHunters: “pay or leak”	https://cybernews.com/security/shinyhunters-claim-vimeo-breach/	T3

Generated 2026-04-29 06:51 UTC by TJS Security Command Center