INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-04 06:08 UTC

ShinyHunters Exploits Okta SSO to Hit Zendesk Instances in Ongoing SaaS Campaign, Hims & Hers Latest Victim

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0145
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Zendesk (customer service platform), Okta (SSO provider); confirmed victims: Hims & Hers Health, ManoMano, Crunchyroll
Published	2026-04-03T13:41:11
Discovery Source	Rss

Executive Summary

ShinyHunters is running an active campaign targeting organizations that use Okta SSO paired with Zendesk, gaining access through compromised Okta credentials and exfiltrating customer support ticket data containing PII. Hims & Hers Health confirmed unauthorized access to its Zendesk environment February 4-7, 2026; ManoMano and Crunchyroll were hit through the same chain. Any organization using Okta to authenticate into Zendesk without enforced MFA and bulk-export controls is exposed to the same attack path today.

Technical Analysis

ShinyHunters is exploiting a multi-weakness attack chain: initial access via compromised Okta SSO cloud accounts (T1078.004, Valid Accounts: Cloud Accounts), likely acquired through phishing (T1566, unconfirmed), followed by lateral movement into downstream Zendesk instances through the trusted SSO relationship. No CVE is assigned; the vulnerability surface is misconfiguration and authentication control gaps, not a discrete software flaw. Relevant CWEs: CWE-287 (Improper Authentication, absent or unenforced MFA on Okta), CWE-306 (Missing Authentication for Critical Function, no bulk export controls in Zendesk), CWE-359 (Exposure of Private Personal Information). Post-access, attackers collected customer support ticket data containing PII via data exfiltration from cloud storage objects (T1530). Application access tokens may have been used to maintain persistence without re-authenticating through Okta (T1550.001). Confirmed victims across three separate February-March 2026 incidents establish a repeating pattern against this specific SSO-to-SaaS

pivot path. No patch is available or applicable; remediation is entirely control-based.

Action Checklist

1. Containment, Revoke suspicious or unrecognized sessions via Okta Admin Console > Sessions immediately. If simultaneous revocation of all Zendesk-connected sessions is operationally infeasible (e.g., production support dependency), instead restrict Zendesk access to a whitelist of known office IPs using Okta network zone policies, monitor for re-entry attempts, and revoke in cohorts during scheduled maintenance windows.
2. Detection, Review Okta System Log for anomalous authentication events: off-hours logins, new device/IP combos, rapid credential reuse across services, and successful logins from locations inconsistent with user baselines. In Zendesk, audit Admin > Audit Log for bulk ticket exports, API token generation, or role changes outside change-control windows. Cross-correlate Okta app access events (event type: app.oauth2.token.grant) with Zendesk API activity timestamps.
3. Eradication, Enforce MFA on all Okta accounts with access to Zendesk, no exceptions for service accounts or shared credentials. Rotate all Okta credentials for Zendesk-connected accounts. Revoke and regenerate Zendesk API tokens. Disable or restrict Zendesk bulk-export functionality to authorized roles only via Zendesk Admin Center > Account > Security > Agent device management and export controls.
4. Recovery, Validate MFA enforcement is active for all affected accounts in Okta via a policy compliance report. Confirm no residual unauthorized API tokens exist in Zendesk. Monitor Okta System Log and Zendesk Audit Log continuously for 30 days post-remediation for re-entry attempts. Notify affected customers per applicable breach notification obligations if PII exposure is confirmed.
5. Post-Incident, This attack exposed three control gaps: absence of phishing-resistant MFA as a likely vector (upgrade to FIDO2/WebAuthn over TOTP where possible per NIST SP 800-63B AAL2/3 guidance if phishing credential acquisition is confirmed), excessive trust in SSO-connected SaaS without downstream access controls, and no alerting on bulk data operations in Zendesk. Implement Okta Workflows or SIEM rules to alert on first-time Zendesk access from new devices. Map SaaS application inventory against SSO trust relationships and apply least-privilege access reviews quarterly.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and privacy officer if Zendesk Audit Log confirms any ticket export or bulk data access during the February 4–7, 2026 window (or any window matching ShinyHunters' campaign TTPs), as exported customer support tickets from health-adjacent organizations like Hims & Hers may contain PHI or PII triggering HIPAA breach notification (60-day clock), CCPA notification obligations, or EU GDPR Article 33 (72-hour supervisory authority notification) depending on affected customer geography.

Recovery Notes	Post-containment, validate recovery by running a full Okta policy compliance check confirming zero Zendesk-connected accounts authenticate without phishing-resistant MFA, and confirm via Zendesk API that no active tokens exist with creation dates predating the remediation action. Maintain heightened monitoring of Okta System Log for `user.authentication.sso` events targeting Zendesk from any IP not in the established corporate allowlist for a minimum of 30 days, as ShinyHunters is an active, persistent threat actor known to re-attempt access after initial eviction. If any re-entry attempt is detected, treat it as a new incident and re-execute containment immediately rather than attempting incremental remediation.
Forensic Artifacts	Okta System Log JSON export (via API: GET /api/v1/logs) filtered to event types user.authentication.sso, app.oauth2.token.grant, user.session.start, and policy.evaluate_sign_on targeting the Zendesk application — primary artifact establishing the credential compromise chain and attacker source IPs used by ShinyHunters | Zendesk Audit Log export (via API: GET /api/v2/audit_logs.json) capturing all ticket_export, api_token_created, bulk_action, and role_change events during the compromise window — directly evidences the data exfiltration phase of this specific SaaS campaign | Okta active session snapshot (Okta Admin Console > Reports > Active Sessions, filtered to Zendesk application) captured before bulk session revocation — preserves sessionId-to-userPrincipalName-to-sourceIP binding that will be destroyed upon revocation and is required to attribute exfiltration actions to specific compromised identities | Zendesk active API token inventory (GET /api/v2/api_tokens.json) with full metadata including created_at timestamps — any token created during the ShinyHunters campaign window not matching a documented provisioning request is direct evidence of attacker persistence mechanism establishment | Okta ThreatInsight or Identity Security Posture Management report (if licensed) or manual Okta System Log pivot on client.ipAddress fields cross-referenced against threat intelligence sources (e.g., GreyNoise, AbuseIPDB) for IPs observed during the compromise window — maps attacker infrastructure to the broader ShinyHunters campaign and may reveal shared IPs with the ManoMano or Crunchyroll intrusions

Per-Action IR Details

Containment — Audit all active Okta SSO sessions connected to Zendesk immediately. Revoke suspicious or unrecognized sessions via Okta Admin Console > Sessions. Temporarily restrict Zendesk access to known trusted IPs using Okta network zone policies if bulk-revoke is not operationally feasible.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), CIS 6.2 (Establish an Access Revoking Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without an enterprise SIEM, use the Okta System Log API directly: run `curl -H 'Authorization: SSWS {apiToken}' 'https://{yourOktaDomain}/api/v1/logs?filter=eventType+eq+"app.oauth2.token.grant"&since={incident_start_ISO8601}'` to pull all Zendesk-targeted token grants. Export to CSV and pivot on `actor.alternateId`, `client.ipAddress`, and `client.geographicalContext.country` to identify anomalous source IPs. For network zone lockdown, use Okta Admin Console > Security > Networks to create an allowlist zone restricted to your known office/VPN egress IPs and assign it to the Zendesk app sign-on policy — no tooling beyond a browser required.

Evidence: Before revoking sessions, export a full snapshot of Okta System Log entries for the Zendesk application covering at minimum February 4–7, 2026 (confirmed Hims & Hers window) plus 72 hours prior. Capture: `sessionId`, `actor.alternateId` (UPN), `client.ipAddress`, `client.userAgent.rawUserAgent`, `client.geographicalContext`, `target[].displayName` (should show Zendesk app), and `authenticationContext.credentialType`. This preserves the session-binding evidence that links compromised Okta credentials to Zendesk access before revocation destroys live session state. Also capture a point-in-time export of Okta > Reports > Active Sessions filtered to the Zendesk application before bulk revocation.

Detection — Review Okta System Log for anomalous authentication events: off-hours logins, new device/IP combos, rapid credential reuse across services, and successful logins from locations inconsistent with user baselines. In Zendesk, audit Admin > Audit Log for bulk ticket exports, API token generation, or role changes outside change-control windows. Cross-correlate Okta app access events (event type: app.oauth2.token.grant) with Zendesk API activity timestamps.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

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 the following two-step manual correlation: (1) Pull Okta System Log via API filtering on `eventType eq "app.oauth2.token.grant" and target.displayName eq "Zendesk"` — export to a flat file. (2) Pull Zendesk Audit Log via `GET /api/v2/audit_logs.json?filter[created_at]={start}:{end}` using a Zendesk Admin API token — export to a second flat file. Join both datasets on timestamp proximity (±5 minute window) using a simple Python pandas merge or even Excel VLOOKUP on rounded timestamps. Flag rows where Okta `client.ipAddress` does not appear in your known-user IP baseline. A two-person team can complete this triage in under two hours using free tooling. Additionally, deploy the public Sigma rule `okta_suspicious_app_access.yml` (available in the SigmaHQ repository) converted to an Okta System Log query format for ongoing manual sweeps.

Evidence: Okta System Log: filter on event types `user.authentication.sso`, `app.oauth2.token.grant`, `user.session.start`, and `policy.evaluate_sign_on` targeting the Zendesk application. Key anomaly fields: `client.ipAddress` originating from non-corporate ASNs, `client.device` showing first-seen device fingerprints, `outcome.reason` values of `SUCCESS` following prior `FAILED` attempts (credential stuffing indicator). Zendesk Audit Log: look for `ticket_export`, `api_token_created`, `role_change`, and `bulk_action` event types — ShinyHunters' SaaS exfiltration pattern relies on bulk ticket export APIs, so any `ticket_export` event from an IP not matching the authenticated Okta session source IP is a high-confidence indicator. Preserve raw JSON from both APIs — do not rely solely on UI-exported CSVs, which may truncate fields.

Eradication — Enforce MFA on all Okta accounts with access to Zendesk — no exceptions for service accounts or shared credentials. Rotate all Okta credentials for Zendesk-connected accounts. Revoke and regenerate Zendesk API tokens. Disable or restrict Zendesk bulk-export functionality to authorized roles only via Zendesk Admin Center > Account > Security > Agent device management and export controls.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: For teams without PAM tooling: enumerate all Zendesk-connected Okta accounts via `GET /api/v1/apps/{zendeskAppId}/users` and pipe output through `jq '.[] | select(.credentials.password != null) | .profile.login'` to identify accounts still using password-only auth. For service accounts that cannot tolerate interactive MFA, migrate them to Okta OAuth 2.0 client credentials flow scoped to minimum required Zendesk API permissions — this eliminates shared-credential risk without requiring human MFA interaction. For Zendesk API token revocation, use `GET /api/v2/api_tokens.json` to list all active tokens, then `DELETE /api/v2/api_tokens/{id}.json` for each — scriptable in a 10-line bash loop with curl. Document each deleted token's `description` field and `created_at` timestamp as evidence that pre-existing unauthorized tokens have been cleared.

Evidence: Before enforcing MFA policy changes, snapshot Okta's current authentication policy for the Zendesk application via `GET /api/v1/apps/{zendeskAppId}/policies` — this documents the pre-incident control gap for regulatory evidence and post-incident review. In Zendesk, export the full active API token list (`GET /api/v2/api_tokens.json`) capturing `id`, `description`, `created_at`, and `active` fields — any token with a `created_at` timestamp falling within February 4–7, 2026 (or the broader campaign window) and not matching a documented change-control record is presumed compromised. Preserve this list before deletion. Also capture Okta's `user.mfa.factor.deactivate` and `user.mfa.factor.reset_all` event log entries to confirm no attacker pre-emptively

disabled MFA on targeted accounts.

Recovery — Validate MFA enforcement is active for all affected accounts in Okta via a policy compliance report. Confirm no residual unauthorized API tokens exist in Zendesk. Monitor Okta System Log and Zendesk Audit Log continuously for 30 days post-remediation for re-entry attempts. Notify affected customers per applicable breach notification obligations if PII exposure is confirmed.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For MFA compliance validation without enterprise tooling: use Okta System Log query `eventType eq "user.mfa.factor.activate"` filtered to the post-remediation window and cross-reference against the full Zendesk-connected user list from `GET /api/v1/apps/{zendeskAppId}/users` — any user not appearing in the activation log who has not previously enrolled is non-compliant. For ongoing 30-day monitoring without a SIEM, configure Okta's built-in System Log streaming to an email or webhook destination (Okta > Security > Log Streaming) and write a simple scheduled script (cron + curl) that daily queries `eventType eq "app.oauth2.token.grant" and target.displayName eq "Zendesk"` and diffs against a known-good IP allowlist, alerting on any new source. For breach notification scoping, query Zendesk Audit Log for all `ticket_export` and `ticket_view` events during the compromise window — output includes ticket IDs, which can be joined against ticket content to assess PII categories exposed (names, emails, health-related support content in the case of Hims & Hers).

Evidence: Retain the full Okta System Log and Zendesk Audit Log covering the February 4–7, 2026 compromise window plus 30 days of post-remediation monitoring — minimum retention per NIST AU-11 (Audit Record Retention) for incident support. For breach notification evidence: export all Zendesk ticket records accessed or exported during the compromise window, preserving ticket metadata (`ticket_id`, `requester_id`, `subject`, `created_at`, `updated_at`) and the associated audit log `actor` field — this establishes which customer records were touched and by which (compromised) agent identity. This dataset is the basis for customer notification scope determination and potential HIPAA/CCPA regulatory filings given Hims & Hers' health-adjacent business context. Worth noting this touches regulatory breach notification obligations — you should verify specific timing and content requirements with qualified legal counsel given the health data context of at least one confirmed victim.

Post-Incident — This attack exposed three control gaps: absence of phishing-resistant MFA (upgrade to FIDO2/WebAuthn over TOTP where possible per NIST SP 800-63B AAL2/3 guidance), excessive trust in SSO-connected SaaS without downstream access controls, and no alerting on bulk data operations in Zendesk. Implement Okta Workflows or SIEM rules to alert on first-time Zendesk access from new devices. Map SaaS application inventory against SSO trust relationships and apply least-privilege access reviews quarterly.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-7 (Software, Firmware, and Information Integrity), NIST RA-3 (Risk Assessment), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For FIDO2/WebAuthn rollout without enterprise budget: Okta's free tier supports WebAuthn enrollment — enable it under Security > Authenticators > Add Authenticator > FIDO2 (WebAuthn) and create a sign-on policy rule requiring it for Zendesk access specifically. For SaaS trust mapping without a CASB: use Okta Admin > Applications > Applications list export (CSV available natively) to enumerate all active SSO-connected apps, then manually annotate each with: data classification of data accessible, whether MFA is enforced on the Okta sign-on policy, and whether the app has bulk-export or API capabilities. This produces a one-page SaaS risk register achievable in a single sprint. For bulk-export alerting without a SIEM: use Zendesk's native trigger system (Admin Center > Objects and Rules > Business Rules > Triggers) to fire a webhook on ticket export events, routing to a free

Slack webhook or email alert — this is zero-cost and requires no external tooling.

Evidence: The lessons-learned deliverable for this incident should include: (1) a documented timeline mapping ShinyHunters' credential acquisition to first Okta authentication to first Zendesk bulk export — derived from the correlated Okta System Log and Zendesk Audit Log evidence collected during detection; (2) a before/after authentication policy export from Okta showing the control gap (MFA not required) and the remediated state; (3) the full list of Zendesk API tokens active during the compromise with creation timestamps, as evidence of the access-control gap that allowed unauthorized token generation; and (4) a SaaS application inventory snapshot documenting which other Okta-connected applications share the same authentication policy as Zendesk — this scopes the lateral risk to other SaaS platforms that ShinyHunters or similar actors could pivot to using the same credential chain.

Detection Guidance

Okta System Log (Admin Console > Reports > System Log or via API /api/v1/logs): query for event types user.session.start and app.oauth2.token.grant filtered to the Zendesk application assignment. Flag: logins from ASNs or countries not in the user's 30-day history, successful authentications without an MFA step (factor_type: null or skipped), and multiple app accesses within seconds of credential entry. Zendesk Audit Log (Admin Center > Account > Audit Log): flag bulk ticket exports (export_all_tickets, search export), API token creation events, and agent role escalations. Behavioral IOC: a single Okta identity authenticating to Zendesk followed within minutes by a large-volume ticket query or export is the primary pattern seen in this campaign. No public IOCs (IPs, domains, hashes) have been confirmed attributed to ShinyHunters in this specific campaign as of the source coverage available.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs publicly attributed to this campaign`	ShinyHunters' TTPs in this campaign rely on valid stolen credentials rather than malware infrastructure. No IPs, domains, or file hashes have been confirmed and attributed in source coverage as of 2026-04-02. Do not populate IOC blocklists from unverified third-party claims.	LOW

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1550.001** — Application Access Token
- **T1078.004** — Cloud Accounts
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1213** — Data from Information Repositories
- **T1114.003** — Email Forwarding Rule

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
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

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

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1550.001	Application Access Token	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1213	Data from Information Repositories	Collection
T1114.003	Email Forwarding Rule	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hims-and-hers-warns-...	T3
Telehealth giant Hims & Hers says its customer support system was ...	https://techcrunch.com/2026/04/02/telehealth-giant-hims-hers-says-i...	T2
Hims & Hers Confirms Customer Support Breach in February	https://www.techbuzz.ai/articles/hims-hers-confirms-customer-suppor...	T3
Hims & Hers Data Breach Exposes Customer Service Records	https://www.claimdepot.com/data-breach/hims-hers-2026	T3
Email Bombs Exploit Lax Authentication in Zendesk	https://krebsonsecurity.com/2025/10/email-bombs-exploit-lax-authent...	T3

Generated 2026-04-04 06:08 UTC by TJS Security Command Center