INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:41 UTC

ManoMano Zendesk Data Breach Allegedly Exposes 38 Million Customer Records

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0026
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	ManoMano customer data hosted via Zendesk (support platform instance); specific Zendesk version not publicly disclosed
Published	2026-02-25

Executive Summary

An unattributed threat actor claims to have exfiltrated personal data belonging to approximately 38 million ManoMano customers from the company's Zendesk customer support instance; ManoMano has not publicly confirmed the breach as of available reporting. ManoMano operates across France, Spain, Italy, Germany, Belgium, and the UK, meaning exposure likely triggers GDPR notification obligations across multiple jurisdictions if the claim is verified. The primary business risk is regulatory liability, customer trust erosion, and potential downstream fraud targeting affected individuals, though the 38 million figure and data authenticity remain unverified pending independent confirmation. Note: source reporting originates from threat actor claims and secondary news coverage; treat as unverified until ManoMano issues an official statement.

Technical Analysis

Alleged unauthorized access to ManoMano's Zendesk SaaS customer support instance resulting in claimed exfiltration of PII for approximately 38 million customers. The specific Zendesk version, tenant configuration, and exact data fields compromised have not been publicly disclosed. Attack vector is unconfirmed but consistent with third-party SaaS exploitation patterns mapped to MITRE ATT&CK T1199 (Trusted Relationship), T1078 (Valid Accounts), T1530 (Data from Cloud Storage), and T1566 (Phishing) as plausible initial access methods. No CVE has been assigned; weakness mapping references CWE-306 (Missing Authentication for Critical Function), CWE-359 (Exposure of Private Personal Information to Unauthorized Actor), and CWE-284 (Improper Access Control). No patch is applicable in the traditional sense, this is a SaaS tenant compromise, not a software vulnerability with a published fix. Zendesk has not issued a platform-wide advisory; if access was via stolen credentials or misconfigured permissions, remediation is configuration and access control dependent.

Source quality score is 0.54 (T3 sources only); no independent forensic verification has been published.

Action Checklist

1. Step 1, Immediate: If your organization uses Zendesk, audit all active admin and agent accounts for unauthorized access; rotate credentials and review API token issuance logs.
2. Step 2, Detection: Review Zendesk audit logs for anomalous bulk data exports, API calls with high record-retrieval volume, or access from unfamiliar IPs or geolocations; cross-reference against normal baseline.
3. Step 3, Assessment: Inventory what customer PII your Zendesk instance holds, ticket content, contact data, attachments, and map exposure scope against your customer base and applicable data residency requirements.
4. Step 4, Communication: If your organization shares Zendesk infrastructure with ManoMano or uses a similar third-party support SaaS model, brief legal and privacy counsel on GDPR Article 33 notification timelines (72-hour clock) in case internal investigation surfaces exposure.
5. Step 5, Long-term: Enforce least-privilege access controls on all third-party SaaS support platforms; implement MFA on all privileged Zendesk roles; schedule periodic access reviews; evaluate data minimization practices to limit PII retention in support tickets.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to incident response leadership and external forensic firm immediately if Zendesk audit logs show evidence of successful data export (record counts > 10k, API calls to /api/v2/tickets?include=users in rapid succession, or IPs geolocated outside your organization's known ranges); escalate to legal/compliance and data protection authority (DPA) if any customer PII (email, phone, address) is confirmed exfiltrated, given GDPR 72-hour notification deadline.
Recovery Notes	Post-containment: implement mandatory MFA and least-privilege role enforcement within 2 weeks. Conduct lessons-learned session within 30 days to document gaps in audit log monitoring and access controls. Execute full access re-certification (audit all Zendesk users against current HR records) within 30 days. If no unauthorized access is confirmed during forensic analysis, document findings and close with compensating control implementation; if unauthorized access is confirmed, extend investigation to linked systems (email, CRM, analytics platforms) that may have received Zendesk data via API integrations.
Forensic Artifacts	Zendesk audit log export (Settings > Audits > Export): action, user, IP, timestamp, object_id, object_type | Zendesk API token issuance log (GET /api/v2/api_tokens): token_id, user_id, created_at, last_used_at | Proxy/firewall access logs for *.zendesk.com and zendesk.com/api: source_ip, destination, timestamp, bytes_transferred, user_agent | Zendesk database transaction logs (if self-hosted) or request logs (if SaaS, via Zendesk support): SELECT/EXPORT operations, record counts, user_id, timestamp | GeoIP and threat intelligence lookup results for anomalous login IPs: geolocation, ASN, known malware C2 infrastructure matches

Per-Action IR Details

Step 1, Immediate: If your organization uses Zendesk, audit all active admin and agent accounts for unauthorized access; rotate credentials and review API token issuance logs.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and processes)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 AC-3 (Access Enforcement), CIS 6.1 (Establish an Access Management Process)

Compensating: Export admin/agent user list via Zendesk API (curl or Postman): GET /api/v2/users?role=admin|agent. Cross-reference against HR onboarding/offboarding records manually. For API tokens, query GET /api/v2/api_tokens and log timestamps. Rotate via Settings > API > Tokens; delete unused tokens immediately. If no API audit trail exists in your instance, document absence as evidence of configuration gap.

Evidence: Capture Zendesk account audit log export (Settings > Audits) before rotating; screenshot all active API tokens with creation/last-used timestamps; export user provisioning records from IdP (AD, Okta, or local Zendesk directory); preserve /var/log/auth.log or Windows Event Log 4624 (logon events) from systems where Zendesk credentials are cached or used.

Step 2, Detection: Review Zendesk audit logs for anomalous bulk data exports, API calls with high record-retrieval volume, or access from unfamiliar IPs or geolocations; cross-reference against normal baseline.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Analysis phase: acquire and analyze artifacts)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Export Zendesk audit logs via Settings > Audits > Export (CSV); filter for action:export_tickets, action:create_api_request, action:bulk_import. Cross-reference agent login IPs against GeoIP database (free: MaxMind GeoLite2) to flag anomalous geography. Baseline normal access by time-of-day, role, and IP range from 90 days of clean logs. Use grep/awk to parse CSV for ticket_count > 10k/hour or export_event_count > 100 in 24h windows. Document any gaps in audit retention (Zendesk default: 30 days).

Evidence: Preserve complete Zendesk audit log export with timestamps, user IDs, IP addresses, and actions; capture browser access logs from proxy/firewall (if available) for all Zendesk URLs (*.zendesk.com, zendesk.com/api); extract 90-day baseline of normal API call patterns (GET /api/v2/tickets counts, export frequency, agent geolocations) for comparison; preserve network flow logs (NetFlow/sflow) showing data volume egress from Zendesk infrastructure.

Step 3, Assessment: Inventory what customer PII your Zendesk instance holds, ticket content, contact data, attachments, and map exposure scope against your customer base and applicable data residency requirements.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Profile normal traffic and behavior); NIST 800-53 SA-3 (System Development Life Cycle) in context of data handling

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 DM-1 (Data Minimization), CIS 3.1 (Establish Data Handling Policy), CIS 13.1 (Maintain an Inventory of Assets)

Compensating: Query Zendesk database schema (if self-hosted) or request data export from Zendesk (Admin > Settings > Data Portability). Scan ticket bodies and custom fields for regex patterns: email (\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Z|a-z]{2,}\b), phone (\+?\d{10,15}), SSN/tax ID, credit card (luhn-check), passport. Use free tool: grep -E for pattern matching, or Python script with re module. Sample 1000 random tickets to estimate PII density. Cross-tabulate against customer database (by account ID) to determine exposure count. Map Zendesk instance geographic residency (EU, US, etc.) against GDPR, CCPA, or local data residency law requirements.

Evidence: Export complete Zendesk data schema and sample of ticket records (anonymized, but preserve counts by PII type); capture custom field definitions and their usage frequency (query GET /api/v2/ticket_fields); preserve Zendesk instance metadata (account creation date, last backup, encryption-at-rest configuration from Admin settings);

document data retention policy (Settings > Security > Data Retention) and any custom integrations that may copy PII elsewhere (Slack, Teams, external CRM).

Step 4, Communication: If your organization shares Zendesk infrastructure with ManoMano or uses a similar third-party support SaaS model, brief legal and privacy counsel on GDPR Article 33 notification timelines (72-hour clock) in case internal investigation surfaces exposure.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment strategy); NIST 800-53 IR-1 (Incident Response Policy)

Controls: NIST 800-53 IR-2 (Incident Response Training), NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-8 (Incident Response Plan), CIS 17.1 (Designate Leadership and Establish Incident Response Readiness)

Compensating: Create a documented timeline log: (1) date/time of breach awareness, (2) date/time of internal investigation start, (3) date/time exposure confirmed, (4) date/time notification to authorities. GDPR Article 33 clock starts at discovery of unauthorized access; send breach notification to supervisory authority (e.g., CNIL for France, ICO for UK) within 72 hours of discovery. Document decision rationale if delay is necessary (legitimate technical investigation). Brief legal on notification template requirements per Article 34 (data subject notification). Do not rely on Zendesk/ManoMano to notify your customers; confirm data controller responsibility in writing.

Evidence: Preserve all communications with Zendesk support, legal team, and data protection authority (email, tickets, meeting notes with timestamps). Maintain a signed incident timeline attestation from legal counsel. Document the basis for determining 'discovery' date (first detection log entry, first report received, first internal escalation). Capture screenshots of breach report templates you prepared for authority submission (proof of timely notification intent).

Step 5, Long-term: Enforce least-privilege access controls on all third-party SaaS support platforms; implement MFA on all privileged Zendesk roles; schedule periodic access reviews; evaluate data minimization practices to limit PII retention in support tickets.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities: lessons learned); NIST 800-53 AC-6 (Least Privilege), AC-5 (Separation of Duties)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-2 (Authentication), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 AU-9 (Protection of Audit Information), CIS 6.2 (Ensure Proper User Access Management), CIS 6.3 (Require MFA for All Users)

Compensating: Zendesk native: configure roles via Admin > Team Members > Roles; assign agent-specific permissions (limit to assigned ticket queues, no global data export). Enable MFA via Settings > Security > Two-Factor Authentication (require for admin/lead roles). Schedule quarterly access reviews: export user list, cross-reference against current org chart, disable unused accounts (curl DELETE /api/v2/users/{id}). For data minimization: disable custom fields that store PII (passport, SSN) unless business-critical; use ticket masking rules to redact sensitive content in search/export. If Zendesk offers no masking, implement compensating control: ticket redaction script (regex filter) before export to third parties.

Evidence: Preserve baseline role configuration (Settings > Roles > export) before and after hardening. Document MFA enrollment status for each privileged user (screenshot from Settings > Two-Factor Authentication). Create a signed access review checklist for each quarterly review (user name, role, last login date, justification for retention, approver signature). Capture data retention policy change log (before/after comparison of Settings > Data Retention). Preserve communication to users explaining MFA and role changes (email receipt proof).

Detection Guidance

Detection applies primarily to organizations running Zendesk or similar SaaS support platforms, not to ManoMano customers directly. Key indicators to investigate: (1) Zendesk audit log entries showing large-scale ticket or user data exports outside normal business hours or by accounts not typically performing exports; (2) API calls with unusually high request volumes against /api/v2/users or /api/v2/tickets endpoints; (3) new OAuth

app authorizations or API token creation events not tied to known change management activity; (4) logins from IP ranges inconsistent with your organization's normal access geography. For organizations monitoring supply chain risk: watch threat intelligence feeds and dark web monitoring services for ManoMano or Zendesk dataset listings as a signal of confirmed data availability. No specific IOCs (IPs, hashes, domains) have been publicly confirmed as associated with this incident as of available reporting, treat any claimed IOCs from unverified sources with caution.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs published`	No specific indicators of compromise have been publicly attributed to this incident as of available reporting. The threat actor advertisement has not been accompanied by verified technical artifacts. Monitor threat intelligence feeds for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1199** — Trusted Relationship
- **T1566** — Phishing

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
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

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

- **A01:2021** — Broken Access Control

CIS-V8

- **6.3**
- **6.1**
- **6.2**
- **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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **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

- **RS.CO-03** — Recovery activities and progress communicated
- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1199	Trusted Relationship	Initial-Access
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
SecurityWeek	https://www.securityweek.com/38-million-allegedly-impacted-by-manom...	T3

Source	URL	Tier
ManoMano Zendesk Data Breach Exposes 38 Million Customers ...	https://www.rescana.com/post/manomano-zendesk-data-breach-exposes-3...	T3
European DYI chain ManoMano data breach impacts 38 million ...	https://www.bleepingcomputer.com/news/security/european-dyi-chain-m...	T3
ManoMano data breach: massive DIY chain incident impacts 38 ...	https://www.techradar.com/pro/security/manomano-data-breach-massive...	T3
38 Million Users Affected by ManoMano Data Breach from ... - Reddit	https://www.reddit.com/r/pwnhub/comments/1rgkpm9/38_million_users_a...	T3

Generated 2026-03-29 18:41 UTC by TJS Security Command Center