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

Aura Identity Protection Platform Breached via Vishing; ShinyHunters Claims Responsibility for 900K Record Exposure

DATA BREACH | MEDIUM | CVSS 5.0

SCC Item ID	SCC-DBR-2026-0051
Type	Data Breach
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Aura (identity protection platform, unspecified version); unnamed acquired marketing tool (third-party); Okta SSO (alleged, unconfirmed by Aura)
Published	2026-03-21

Executive Summary

Aura, a consumer identity protection platform, confirmed a data breach after an employee fell victim to a vishing attack, granting unauthorized access to a third-party marketing database. Approximately 900,000 records were exposed; roughly 35,000 belong to current Aura customers. Sensitive identity data (SSNs, passwords) were not reported as compromised, but ShinyHunters has published the stolen data following failed ransom negotiations, raising phishing and fraud risk for affected individuals.

Technical Analysis

Attack vector: Voice phishing (vishing) targeting an Aura employee, mapped to MITRE T1566.004 (Phishing: Spearphishing Voice) and T1598.004. The attacker leveraged social engineering to obtain credentials or access (CWE-287: Improper Authentication), gaining entry to a marketing database associated with an acquired third-party marketing tool. Exposed data fields include names, email addresses, and phone numbers across approximately 900,000 records. An Okta SSO compromise has been alleged (T1078: Valid Accounts), consistent with ShinyHunters' documented TTPs in prior campaigns, but remains unconfirmed by Aura. Data exfiltration aligns with T1530 (Data from Cloud Storage) and T1657 (Financial Extortion). Attribution to ShinyHunters is self-claimed; the group published the dataset after ransom negotiations failed. No CVE is assigned. Relevant CWEs: CWE-287 (Improper Authentication), CWE-1059 (Insufficient Documentation of Error Handling), CWE-359 (Exposure of Private Personal Information). No patch is applicable; this is a social engineering and access control failure, not a software vulnerability. The compromised marketing tool and its version remain unidentified publicly.

Action Checklist

1. Step 1, Immediate: Audit employee access to third-party marketing platforms and any tools acquired through M&A activity; revoke or rotate credentials for any accounts with access to marketing or CRM databases.
2. Step 2, Detection: Review SSO and identity provider logs (especially Okta if in use) for anomalous authentication events, particularly successful logins preceded by unusual MFA prompts or out-of-hours access in the relevant timeframe; query for T1078 indicators.
3. Step 3, Assessment: Inventory all third-party tools obtained through acquisitions; confirm whether any share authentication infrastructure with core systems; identify which internal databases contain PII accessible via marketing or analytics tooling.
4. Step 4, Vishing Awareness: Issue a targeted staff advisory on vishing TTPs; remind employees of callback verification procedures before granting system access or credentials over voice channels; confirm help desk and IT support anti-vishing protocols are current.
5. Step 5, Long-term Controls: Implement or enforce phishing-resistant MFA (e.g., FIDO2/passkeys) on SSO and marketing platforms; establish data minimization standards for acquired tool integrations; add vishing simulation to security awareness training cadence per NIST SP 800-50 guidance.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm and law enforcement (FBI IC3) immediately if forensic analysis in Step 2 reveals evidence of persistent lateral movement into core systems beyond the marketing platform, or if Step 3 inventory identifies that compromised marketing tool databases were synchronized with customer PII systems; vishing incidents involving successful SSO compromise warrant disclosure legal review given identity data exposure.
Recovery Notes	Post-containment recovery: (1) After credential rotation (Step 1) and detection analysis confirms scope (Step 2), reset all affected user passwords and revoke all active sessions in Okta; force re-authentication with new MFA methods; (2) For the acquired marketing tool, shut down the vulnerable instance, restore from clean backup (validated against timeline), re-deploy with network isolation and restricted database access (Step 3); (3) Notify affected customers (900K records per advisory) with breach notification letter per state law requirements (typically 30–60 days); provide 24-month credit monitoring and identity theft protection. Document all recovery actions with timestamps and approvals for regulatory reporting.

Forensic Artifacts	Okta System Log (60-day export) — event types: user.authentication.auth_via_okta, user.mfa.attempt_bypass, policy.evaluate_sign_on, user.session.start, user.session.end | Windows Event Viewer: Security log (Event ID 4624/4625 for successful/failed logons; 4768/4769 for Kerberos TGT requests; 4672 for privilege use) and application logs from SSO/IdP services | Linux /var/log/auth.log and /var/log/secure — authentication attempts, sudo usage, service authentication (sshd, PAM modules) | Marketing platform application logs (database connection logs, authentication events, user activity logs) and database audit trails (PostgreSQL pg_stat_statements, MySQL general_log, SQL Server audit tables) | VPN/bastion host access logs with source IP, username, timestamp, and connection duration; network flow data (NetFlow v9, sFlow, or Zeek logs) showing connections to marketing tool infrastructure

Per-Action IR Details

Step 1 — Immediate: Audit employee access to third-party marketing platforms and any tools acquired through M&A activity; revoke or rotate credentials for any accounts with access to marketing or CRM databases.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Control), CIS 6.1 (Establish an Access Management Process), CIS 6.2 (Establish privileged access management)

Compensating: Without privileged access management (PAM) tools, manually query Active Directory for group membership (`Get-ADGroupMember -Identity "[marketing-tool-access-group]" -Recursive` on Windows; `id -Gn [username]` on Linux); cross-reference against employee roster; document findings in a spreadsheet with timestamp; use `passwd -e [username]` (Linux) or force password change at next logon via Active Directory Users and Computers (Windows) for affected accounts. For SaaS platforms (Okta, marketing tools), export access logs via admin console and revoke sessions manually through each vendor's UI.

Evidence: Capture before revocation: (1) Active Directory group membership exports via `Get-ADGroup -Filter * | Export-Csv ad_groups_[timestamp].csv` with membership lists; (2) SaaS platform access audit logs (Okta system log, marketing tool admin audit trail) exported as CSV/JSON; (3) VPN/bastion logs showing authentication attempts to marketing platforms over 90 days prior (Windows Event Log 4624/4625 for local auth, `/var/log/auth.log` for SSH); (4) browser history from employee workstations (Chrome: `%APPDATA%\Google\Chrome\User Data\Default\History`; Firefox: `~/.mozilla/firefox/[profile]/places.sqlite`). Chain of custody: timestamp each export, hash with `sha256sum` (Linux) or `certUtil -hashfile [file] SHA256` (Windows), document who extracted and when.

Step 2 — Detection: Review SSO and identity provider logs (especially Okta if in use) for anomalous authentication events, particularly successful logins preceded by unusual MFA prompts or out-of-hours access in the relevant timeframe; query for T1078 indicators.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Detection and Analysis)

Controls: NIST 800-53 AU-12 (Audit Generation), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.5 (Implement and maintain centralized log management), CIS 8.8 (Implement User and Entity Behavior Analytics)

Compensating: Without SIEM, export Okta system logs manually via Admin Console > Reports > System Log; filter for event types `user.authentication.auth_via_okta` and `user.authentication.authenticate_with_password` with `outcome=SUCCESS`; export to CSV; cross-reference timestamps with office hours (assume 0800–1800 weekdays if no policy available) and identify out-of-hours successes. For acquired marketing tools without native logging, query database connection logs from the application server: check PostgreSQL `log_connections=on` logs in `/var/log/postgresql/` or MySQL slow query log with authentication events. Search for multiple failed MFA attempts followed by success (pattern: event type `user.mfa.attempt_bypass` or equivalent). Use grep to query auth logs: `grep -i "mfa\|okta\|sso" /var/log/auth.log | awk '$3>"180000" || $3<"080000" {print}'` to isolate out-of-hours events.

Evidence: Preserve before analysis: (1) Okta system log export covering 60 days prior to vishing incident (requested date: obtain from Okta support or admin console); (2) MFA provider logs if not Okta-native (e.g., Duo Security Admin API export); (3) acquired marketing tool application logs (typically in `/var/log/[app-name]/` or Windows Event Viewer Application log); (4) VPN access logs with source IP, username, timestamp, and duration for employees accessing marketing platforms; (5) network flow data (NetFlow or Zeek logs) showing connections from external IPs to marketing tool servers during suspected compromise window. Hash each log file and document retrieval timestamp.

Step 3 — Assessment: Inventory all third-party tools obtained through acquisitions; confirm whether any share authentication infrastructure with core systems; identify which internal databases contain PII accessible via marketing or analytics tooling.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Detection and Analysis); NIST SP 800-53 CA-7 (Continuous Monitoring)

Controls: NIST 800-53 CA-6 (Security Categorization), NIST 800-53 CM-8 (Information System Component Inventory), CIS 2.1 (Establish and maintain a hardware asset inventory), CIS 4.1 (Establish and maintain a Software Asset Inventory)

Compensating: Manually audit M&A tool integrations: (1) query IT ticketing system and procurement records for all acquisitions (past 5 years); (2) contact engineering and product teams to document which acquired tools authenticate via shared SSO infrastructure (check Okta application roster in Admin Console > Applications); (3) for each acquired tool, interview administrators to identify data sources—run SQL queries against internal databases to confirm what PII fields are accessible (e.g., `SELECT COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA='[acquired_tool_db]' AND COLUMN_NAME IN ('ssn','email','phone','address');` on MySQL/SQL Server); (4) document in a spreadsheet: tool name, acquisition date, authentication method (SSO/local), database connections, and PII fields exposed. Use `dig` or `nslookup` to resolve marketing tool hostnames and cross-check against internal network segmentation (confirm if on isolated VLAN or mixed with core infrastructure).

Evidence: Capture before remediation: (1) screenshot of Okta Applications list with all configured apps and authentication bindings; (2) system architecture diagrams (physical and logical) showing data flows between acquired tools and core databases; (3) database schema exports (`mysqldump -u [user] --no-data [database] > schema_[timestamp].sql`) showing table structure and PII fields; (4) firewall rules governing traffic between marketing tools and core systems (`iptables -L -n -v > firewall_rules_[timestamp].txt` on Linux; Get-NetFirewallRule on Windows); (5) IAM role/permission audit for all service accounts with access to both acquired tools and core databases (Active Directory, AWS IAM, or equivalent). Hash and timestamp all exports.

Step 4 — Vishing Awareness: Issue a targeted staff advisory on vishing TTPs; remind employees of callback verification procedures before granting system access or credentials over voice channels; confirm help desk and IT support anti-vishing protocols are current.

NIST Phase: Preparation

Reference: NIST 800-61r3 §3.1 (Preparation); NIST SP 800-50 (Security Awareness and Training)

Controls: NIST 800-53 AT-3 (Role-Based Security Training), NIST 800-53 PS-6 (Access Termination), CIS 17.7 (Train workforce members on awareness of physical and information security threats and procedures), CIS 17.8 (Train workforce members on appropriate response to social engineering attempts)

Compensating: Create and distribute a one-page vishing advisory (PDF or internal wiki) covering: (1) vishing definition and red flags (e.g., unsolicited requests for credentials, caller ID spoofing, urgency tactics); (2) callback procedure: always hang up and call back to the official number from company directory or official website, never use a number provided by the caller; (3) escalation path: employees uncertain about requests should contact IT security ([security-email]) with the caller's name/number and context; (4) help desk protocol: IT staff must never request passwords over voice channels—confirm all password resets via out-of-band method (email, SMS code, in-person verification); (5) real example from this incident (anonymized: 'Employee received call claiming to be from IT, asking for Okta credentials to "update access" — this is always a red flag'). Document training completion via email confirmation or LMS attestation. No fancy tools required.

Evidence: Document before distribution: (1) baseline vishing awareness assessment (survey 20–30 random employees: 'Would you give your password to IT over the phone if they asked?' — establish baseline compliance

percentage); (2) help desk ticket logs from past 90 days to identify if other social engineering attempts were reported (query help desk system for keywords 'vishing', 'credential request', 'urgent access'); (3) call recording samples from phone system (if retained) covering the suspected vishing incident window to analyze caller tactics and TTPs. Preserve employee feedback after training rollout (email replies or LMS completion records) as evidence of awareness escalation.

Step 5 — Long-term Controls: Implement or enforce phishing-resistant MFA (e.g., FIDO2/passkeys) on SSO and marketing platforms; establish data minimization standards for acquired tool integrations; add vishing simulation to security awareness training cadence per NIST SP 800-50 guidance.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.2.5 (Recovery); NIST SP 800-63B (Authentication and Lifecycle Management)

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), NIST 800-53 SC-7 (Boundary Protection), CIS 5.2 (Ensure User ID and Authentication Management Policies and Procedures Are Defined and Documented), CIS 6.3 (Require MFA for all remote access of internal network resources and personal devices)

Compensating: Immediate low-cost alternatives: (1) FIDO2—no budget required to enforce on Okta (Okta Verify includes phishing-resistant push auth; YubiKey 5Ci ~$50/unit, compatible with Okta, can be provisioned to high-risk roles first); for marketing platforms, check if vendor supports WebAuthn/FIDO2 natively (many SaaS tools now do via OAuth2 providers); (2) data minimization—audit database access policies: create separate read-only database views for acquired tools, limiting exposure to necessary fields only (`CREATE VIEW marketing_tool_safe AS SELECT email, name FROM customer_db WHERE NOT ssn IS NULL;` — do NOT expose SSN/payment data); document policy in internal data governance wiki; (3) vishing simulation—use free tools (Gophish, Evilginx2 for testing; request security testing approval first) or contract a vendor for quarterly phishing/vishing drills (cost: ~$2–5K/year for mid-market). Track simulation results: % of employees who report simulated calls, % who provide credentials, trend over time. Include vishing scenarios in annual security awareness training (use NIST SP 800-50 templates).

Evidence: Measure and preserve post-implementation: (1) FIDO2 adoption baseline—capture Okta MFA policy report showing % of users with phishing-resistant authenticators enrolled before and 90 days after rollout; (2) vishing simulation results—document all simulation campaigns with employee response data (% reported, % clicked, % provided info), timestamped; (3) data minimization audit—export table schemas and associated view definitions showing PII field restrictions for acquired tools; (4) help desk training attestation—LMS or email records confirming 100% of IT/help desk staff reviewed anti-vishing callback procedures; (5) network segmentation validation—repeat firewall rule audit (Step 3) to confirm marketing tools are isolated from core databases post-remediation. Use these metrics for quarterly security posture reporting.

Detection Guidance

No IOCs (IPs, domains, hashes) have been publicly confirmed for this incident. Detection should focus on behavioral and access anomalies. In Okta or equivalent SSO logs, look for: authentication events from unfamiliar geographies or ASNs, MFA push fatigue patterns (repeated prompts within short windows), and successful logins immediately following failed attempts. In marketing platform audit logs, look for bulk data exports or API calls pulling large record sets outside normal business hours. If your organization uses a third-party marketing tool acquired through M&A, confirm whether its authentication is federated to your SSO; if yes, treat it as in-scope for your identity threat monitoring. Monitor threat intelligence feeds for ShinyHunters data releases; the group has a documented history of posting stolen datasets on hacking forums. Employee-reported suspicious calls claiming to be IT support or vendors are a primary behavioral indicator for vishing campaigns targeting this TTP (T1566.004).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available`	ShinyHunters has published the stolen dataset, but no specific IPs, domains, or file hashes tied to the Aura breach have been publicly confirmed in available sources as of this report. Monitor threat intelligence feeds for emerging indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1566.004** — Spearphishing Voice
- **T1530** — Data from Cloud Storage
- **T1598.004** — Spearphishing Voice
- **T1566** — Phishing
- **T1657** — Financial Theft
- **T1586.002** — Email Accounts
- **T1078** — Valid Accounts

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**
- **6.4**
- **6.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.004	Spearphishing Voice	Initial-Access
T1530	Data from Cloud Storage	Collection
T1598.004	Spearphishing Voice	Reconnaissance
T1566	Phishing	Initial-Access
T1657	Financial Theft	Impact
T1586.002	Email Accounts	Resource-Development
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/aura-confirms-data-b...	T3
No, the Aura Data Breach Did Not Expose Your SSN or ... - PCMag	https://www.pcmag.com/news/no-the-aura-data-breach-did-not-expose-y...	T3

Source	URL	Tier
Security Firm Aura Discloses Data Breach Impacting 900,000 Records	https://www.securityweek.com/security-firm-aura-discloses-data-brea...	T3
Aura data breach: What happened and how to stay protected	https://lifelock.norton.com/learn/data-breaches/aura-data-breach?sr...	T3
The Company Paid to Protect Your Identity Just Got Hacked - Gizmodo	https://gizmodo.com/the-company-paid-to-protect-your-identity-just-...	T3

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