INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 19:05 UTC

# Salesforce Data Exfiltration via Klue OAuth Integration Compromise

DATA BREACH | HIGH | CVSS 8.1

| | |
|---|---|
| SCC Item ID | SCC-DBR-2026-0182 |
| Type | Data Breach |
| Severity | HIGH |
| CVSS Base Score | 8.1 |
| Affected Products | Salesforce (REST API); Klue Battlecards third-party integration |
| Published | 2026-06-18 |
| Discovery Source | Gemini |

## Executive Summary

Threat actors compromised Klue's Battlecards integration service accounts and used stolen OAuth tokens to extract customer records from connected Salesforce instances, without ever obtaining Salesforce credentials directly. Organizations that authorized Klue's OAuth integration with Salesforce are potentially affected, including managed service providers (MSPs) confirmed impacted by Huntress's independent investigation. The core business risk is unauthorized CRM data exfiltration through a trusted third-party channel, a supply chain attack vector that bypasses traditional perimeter controls.

## Technical Analysis

Attackers compromised Klue Battlecards integration service accounts and abused long-lived OAuth tokens to authenticate against the Salesforce REST API as a trusted third-party application. No direct Salesforce tenant credential compromise was required. The attack exploits overprivileged OAuth grants, a pattern mapped to CWE-287 (Improper Authentication), CWE-441 (Unintended Proxy or Intermediary), and CWE-269 (Improper Privilege Management). MITRE ATT&CK techniques involved: T1550.001 (Use Alternate Authentication Material: Application Access Token), T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain), T1078.004 (Valid Accounts: Cloud Accounts), and T1530 (Data from Cloud Storage). No CVE has been assigned. Salesforce reportedly disabled the Klue integration in response. Exfiltrated data includes Salesforce customer records. Patch status: no vendor patch applies, the attack vector is OAuth grant abuse, not a software vulnerability. Remediation requires OAuth token revocation and integration access review. Sources include Huntress incident report, ReliaQuest threat spotlight, and Salesforce status page.

## Action Checklist

1. Step 1: Containment, Immediately audit all connected OAuth applications in your Salesforce org via Setup > Connected Apps OAuth Usage. Revoke OAuth tokens for the Klue Battlecards integration if present. If Salesforce has not already disabled the integration in your tenant, revoke it manually. Confirm no active sessions remain under Klue service account identities. Reference: Salesforce Status Page (status.salesforce.com/generalmessages/20000257).
2. Step 2: Detection, Query Salesforce Event Monitoring logs for REST API calls authenticated via OAuth tokens associated with Klue. Look for bulk SOQL queries, large record exports, or API calls outside business hours from third-party OAuth app identifiers. Review Setup Audit Trail for any Connected App changes. Cross-reference AU-2 (Event Logging) requirements, confirm Salesforce API event logs are enabled and retained per AU-11. Check Huntress blog IOC indicators for MSP-environment specifics.
3. Step 3: Eradication, Revoke all OAuth tokens granted to Klue Battlecards. Review and revoke any other third-party OAuth integrations that hold Read or ReadWrite permissions on Salesforce customer record objects (Account, Contact, Lead, Opportunity). Apply least-privilege OAuth scopes to all remaining integrations per AC-6 (Least Privilege). Remove or restrict service accounts tied to Klue from all Salesforce profiles and permission sets.
4. Step 4: Recovery, After token revocation, re-audit connected app usage via Salesforce Setup > OAuth Usage by User. Confirm no residual sessions exist. Enable Salesforce Shield Event Monitoring or equivalent API call logging if not already active. Validate that remaining integrations are scoped to minimum necessary objects and fields. Monitor for anomalous REST API volume for 30 days post-remediation per AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident, Conduct a full OAuth integration inventory across all SaaS platforms, not just Salesforce, applying CIS 2.1 (Establish and Maintain a Software Inventory) to third-party integrations. Implement a formal OAuth grant review process requiring documented business justification and quarterly revalidation. Map control gaps against AC-20 (Use of External Systems) and AC-6 (Least Privilege). Engage your MSP or CRM administrator to assess whether customer data exfiltrated requires breach notification under applicable regulations.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to legal counsel and executive leadership immediately if Salesforce EventLogFile API event logs confirm that Account, Contact, Lead, or Opportunity records containing PII or regulated data were returned by Klue OAuth API calls, triggering breach notification assessment under GDPR, CCPA, or applicable state privacy laws — particularly for MSP environments where the blast radius extends to multiple downstream customer tenants. |

| | |
|---|---|
| **Recovery Notes** | Post-revocation verification must confirm zero active Klue OAuth sessions across all Salesforce orgs, including any sandbox or developer environments that shared the same Connected App OAuth credentials, as these are commonly overlooked. Monitor Salesforce EventLogFile API event logs daily for 30 days for any re-emergence of high-volume SOQL queries against CRM record objects from newly authorized third-party apps, which may indicate the threat actor pivoted to a different OAuth integration after Klue tokens were revoked. For MSP environments confirmed impacted per Huntress's investigation, treat each managed tenant as a separate incident scope requiring independent log review and breach notification assessment. |
| **Forensic Artifacts** | Salesforce EventLogFile API event logs (event types: 'API', 'Login', 'ConnectedApplication', 'URI') for the 90 days prior to detection — these contain CLIENT_ID (Klue's OAuth app identifier), NUM_ROWS_FETCHED, SOQL query text, source IP, and timestamp, directly evidencing the scope and volume of CRM record exfiltration via the Klue OAuth integration. \| Salesforce Setup Audit Trail (downloadable CSV, 180-day retention) — records any Connected App creation, modification, scope changes, or permission set assignments tied to the Klue Battlecards integration, establishing the timeline of when Klue OAuth access was granted and whether any escalation of privileges occurred. \| Salesforce OAuth Usage by User report snapshot (Setup > OAuth Usage by User) captured before token revocation — preserves the list of active Klue session tokens, associated Salesforce user accounts, last activity timestamps, and granted OAuth scopes at the moment of incident response. \| Salesforce Login History records filtered on APPLICATION_TYPE = 'Connected App' and CLIENT_ID matching Klue's registered OAuth application — provides source IP geolocation and authentication timestamps to determine whether access originated from Klue's expected infrastructure or from attacker-controlled endpoints after credential theft. \| Huntress-published IOC list for MSP-environment specifics (referenced in their independent investigation blog post) cross-referenced against Salesforce org IDs, Connected App CLIENT_IDs, and service account usernames present in your EventLogFile API logs — essential for MSP tenants to confirm whether their specific org was among those accessed. |

### Per-Action IR Details

**Step 1: Containment — Immediately audit all connected OAuth applications in your Salesforce org via Setup > Connected Apps OAuth Usage. Revoke OAuth tokens for the Klue Battlecards integration if present. If Salesforce has not already disabled the integration in your tenant, revoke it manually. Confirm no active sessions remain under Klue service account identities. Reference: Salesforce status notice 20000257.**

**NIST Phase:** Containment

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

**Controls:** NIST AC-12 (Session Termination), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** Export the Salesforce Connected Apps OAuth Usage page as a CSV using Salesforce CLI: `sf org list auth` to enumerate all authenticated sessions, then use the Salesforce REST API endpoint `GET /services/oauth2/token/revoke` with each Klue-associated access token to programmatically revoke. For MSP environments managing multiple Salesforce orgs, loop through each org alias in a bash script using `sf org list --json` and cross-check for 'Klue' in the connected app name field.

**Evidence:** Before revoking tokens, capture a full snapshot of active OAuth sessions via Salesforce Setup > OAuth Usage by User (export to CSV) and query the EventLogFile object for LoginHistory and ApiEvent logs: `SELECT Id, EventType, LogDate FROM EventLogFile WHERE LogDate = LAST_N_DAYS:7 AND EventType IN ('Login','API')`. This preserves the list of active Klue session identifiers, token issuance timestamps, and source IP addresses that will be destroyed upon revocation — critical for determining the window of unauthorized access.

**Step 2: Detection — Query Salesforce Event Monitoring logs for REST API calls authenticated via OAuth tokens associated with Klue. Look for bulk SOQL queries, large record exports, or API calls outside business hours from third-party OAuth app identifiers. Review Setup Audit Trail for any Connected App changes. Cross-reference AU-2 (Event Logging) requirements — confirm Salesforce API event logs are enabled and retained per AU-11. Check Huntress blog IOC indicators for MSP-environment specifics.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, use Salesforce's built-in EventLogFile API directly via curl or Postman: `curl https://.salesforce.com/services/data/v59.0/query?q=SELECT+LogFile+FROM+EventLogFile+WHERE+EventType='API'+AND+LogDate=LAST_N_DAYS:30 -H 'Authorization: Bearer '`. Download the CSV log files and pipe through `grep -i 'klue'` or filter on the CONNECTED_APP_NAME field for Klue identifiers. For bulk SOQL detection, filter rows where NUM_ROWS_FETCHED exceeds 500 or REQUEST_SIZE_BYTES exceeds 1MB, which are indicators of mass Account/Contact/Lead/Opportunity object exfiltration in this threat scenario.

**Evidence:** Capture Setup Audit Trail (Setup > Setup Audit Trail > Download) covering the past 180 days before any changes are made — this records Connected App creation, modification, and permission set changes tied to the Klue integration. Also preserve the EventLogFile entries for event types 'API', 'Login', 'ConnectedApplication', and 'URI' for the Klue OAuth app's CLIENT_ID, as these are the primary forensic record of which Salesforce objects (Account, Contact, Lead, Opportunity) were queried and how many records were returned per API call.

**Step 3: Eradication — Revoke all OAuth tokens granted to Klue Battlecards. Review and revoke any other third-party OAuth integrations that hold Read or ReadWrite permissions on Salesforce customer record objects (Account, Contact, Lead, Opportunity). Apply least-privilege OAuth scopes to all remaining integrations per AC-6 (Least Privilege). Remove or restrict service accounts tied to Klue from all Salesforce profiles and permission sets.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** Use Salesforce CLI to enumerate all Connected Apps and their granted scopes: `sf data query --query "SELECT ConnectedApplicationId, UserId, Scope FROM PermissionSetAssignment" --target-org `. For each remaining integration, use the Salesforce Setup UI to manually inspect OAuth scopes under Setup > Connected Apps > Manage and restrict scopes to the minimum required, removing 'full' and 'api' scopes where only 'chatter_api' or object-specific access is needed. Document each integration's business owner in a spreadsheet before revoking to avoid re-granting undocumented access.

**Evidence:** Before removing Klue service accounts from Salesforce profiles and permission sets, export the current permission set assignments: `SELECT AssigneeId, PermissionSetId, Assignee.Name FROM PermissionSetAssignment WHERE AssigneeId IN (SELECT Id FROM User WHERE Name LIKE '%Klue%')`. This preserves the exact scope of access the Klue service accounts held at time of incident — essential for breach scope determination and regulatory notification if Account, Contact, or Lead records containing PII were accessible. Capture this before any profile or permission set changes alter the live authorization state.

**Step 4: Recovery — After token revocation, re-audit connected app usage via Salesforce Setup > OAuth Usage by User. Confirm no residual sessions exist. Enable Salesforce Shield Event Monitoring or equivalent API call logging if not already active. Validate that remaining integrations are scoped to minimum necessary objects and fields. Monitor for anomalous REST API volume for 30 days post-remediation per AU-6 (Audit Record Review, Analysis, and Reporting).**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AC-17 (Remote Access)

**Compensating:** Without Salesforce Shield, enable the free EventLogFile API (available in Developer and Enterprise editions for 24-hour log retention) and schedule a daily cron job or Task Scheduler job to pull and archive API event logs: `curl .../services/data/v59.0/query?q=SELECT+LogFile+FROM+EventLogFile+WHERE+EventType='API'+AND+LogDate=YESTERDAY`. Store locally and run a daily diff script comparing API call volumes per connected app against the 30-day pre-incident baseline to detect any re-establishment of Klue-like OAuth access patterns or new high-volume SOQL queries against CRM record objects.

**Evidence:** Post-revocation, the primary verification artifact is a clean OAuth Usage by User report (Setup > OAuth Usage by User) showing zero active sessions for any app with 'Klue' in its name or CLIENT_ID matching Klue's registered OAuth application identifier. Additionally confirm that Salesforce Login History shows no successful OAuth logins from Klue's known source IP ranges or service account usernames for the 72-hour window following revocation — any entry in this period indicates token refresh succeeded and revocation was incomplete.

**Step 5: Post-Incident — Conduct a full OAuth integration inventory across all SaaS platforms, not just Salesforce, applying CIS 2.1 (Establish and Maintain a Software Inventory) to third-party integrations. Implement a formal OAuth grant review process requiring documented business justification and quarterly revalidation. Map control gaps against AC-20 (Use of External Systems) and AC-6 (Least Privilege). Engage your MSP or CRM administrator to assess whether customer data exfiltrated requires breach notification under applicable regulations.**

**NIST Phase:** Post Incident

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

**Controls:** NIST AC-20 (Use Of External Systems), NIST AC-6 (Least Privilege), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** For MSPs managing multiple tenants without a centralized SaaS management platform, build an OAuth integration inventory using a shared spreadsheet populated by querying each Salesforce org's ConnectedApplication object: `SELECT Name, OptionsAllowAdminApprovedUsersOnly, StartURL FROM ConnectedApplication`. Extend the same manual review to Microsoft 365 (via Azure AD > Enterprise Applications), Google Workspace (Admin Console > Security > API Controls), and any other SaaS platform where Klue or similar battlecard/competitive intelligence tools were authorized, as this attack class — compromised third-party OAuth integration — is not limited to Salesforce.

**Evidence:** The primary post-incident artifact for breach notification assessment is the intersection of (a) the Salesforce EventLogFile API event logs identifying which object types (Account, Contact, Lead, Opportunity) and how many records were returned per Klue OAuth API call, and (b) the field-level schema for those objects to determine whether PII, PHI, or regulated financial data fields (e.g., Email, Phone, SSN, revenue figures) were included in the SOQL SELECT clauses. Preserve these log exports in immutable storage (write-once S3 bucket or equivalent) for regulatory hold pending breach notification determination.

## Detection Guidance

Primary log source: Salesforce Event Monitoring, specifically the API Event Log File and Login Event Log File, accessible via the Salesforce EventLogFile object. Query for OAuth-authenticated REST API calls where ConnectedAppName matches 'Klue' or 'Klue Battlecards'. Flag bulk record retrieval events: SOQL queries returning more than 200 records in a single call, or total API call volume from the Klue app exceeding your established baseline. Look for LOGIN_KEY values associated with service accounts rather than named users, particularly during off-hours. Secondary source: Salesforce Setup Audit Trail, review for Connected App modifications, permission set changes, or profile assignments made in the period preceding the reported incident. Behavioral indicator: legitimate CRM integrations request records for specific accounts on demand;

exfiltration patterns show broad object queries (SELECT * FROM Contact LIMIT 50000) with no corresponding user-initiated workflow. D3FEND countermeasure D3-UAP (User Account Permissions), audit OAuth app permission scopes and restrict to minimum required objects. D3-LAM (Local Account Monitoring), extend monitoring to service account identities used by integrations.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `https://www.huntress.com/blog/klue-breach-investigation` | Huntress incident investigation blog — contains environment-specific IOC details and MSP impact confirmation; review for indicators relevant to your tenant | HIGH |
| URL | `https://reliaquest.com/blog/threat-spotlight-integration-abused-in-crm-data-theft` | ReliaQuest threat spotlight on the Klue/Salesforce OAuth abuse pattern — includes behavioral indicators and detection recommendations | HIGH |

## Framework Mappings

### MITRE-ATTACK

- **T1550.001** — Application Access Token
- **T1195.002** — Compromise Software Supply Chain
- **T1078.004** — Cloud Accounts
- **T1530** — Data from Cloud Storage

### NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-6** — Least Privilege
- **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** — Require MFA for Externally-Exposed Applications

- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **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

### HIPAA-SECURITY

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

### NIST-CSF-2

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

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1550.001 | Application Access Token | Defense-Evasion |
| T1195.002 | Compromise Software Supply Chain | Initial-Access |
| T1078.004 | Cloud Accounts | Defense-Evasion |
| T1530 | Data from Cloud Storage | Collection |

## Sources

| Source | URL | Tier |
|---|---|---|
| **20000257 - Salesforce Status** | https://status.salesforce.com/generalmessages/20000257 | T3 |
| **Salesforce Data Impacted for Many Victims, including Huntress : r/msp** | https://www.reddit.com/r/msp/comments/1u91ax4/cybercrime_breaches_k... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Klue Integration Abused in Salesforce Data Theft - ReliaQuest** | https://reliaquest.com/blog/threat-spotlight-integration-abused-in-... | T3 |
| **OAuth Hacks Return: Salesforce Disables Third-Party App as CRM ...** | https://www.salesforceben.com/another-oauth-hack-salesforce-disable... | T3 |
| **Cybercrime Breaches Klue: Salesforce Data Impacted for ... - Huntress** | https://www.huntress.com/blog/klue-breach-investigation | T3 |



Generated 2026-06-18 19:05 UTC by TJS Security Command Center