INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-22 06:22 UTC

Icarus Threat Actor Exploits Klue OAuth Tokens to Breach Multiple Salesforce Environments

DATA BREACH | **HIGH** | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0191
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Klue (OAuth tokens for customer Salesforce integrations); downstream victims include Recorded Future, Tanium, Jamf, Sprout Social, Gong, and Insurity (Salesforce data exfiltration)
Published	2026-06-20
Discovery Source	Gemini

Executive Summary

Threat actor group Icarus stole OAuth tokens from Klue, a competitive intelligence SaaS platform, by compromising a legacy credential in Klue's environment. The stolen tokens provided persistent, credential-less access to customer Salesforce environments, resulting in confirmed data exfiltration at six downstream organizations including Recorded Future, Tanium, Jamf, Sprout Social, Gong, and Insurity. The business risk is significant: any organization that integrated Salesforce through Klue may have had CRM data, including customer records, sales pipeline information, and contact data, accessed without authorization.

Technical Analysis

Icarus obtained initial access via a compromised legacy credential in Klue's environment, then stole OAuth tokens used to authenticate Klue's Salesforce integrations on behalf of customer organizations. OAuth token theft (MITRE T1528) allowed the actor to authenticate directly to downstream Salesforce instances without requiring individual account credentials (T1550.001, Application Access Token). The attack propagated across Klue's customer base through the trusted third-party integration channel (T1199, Trusted Relationship), enabling email and cloud storage collection (T1114) across at least six confirmed victim organizations. No CVE has been assigned. Relevant weaknesses include CWE-272 (Least Privilege Violation), CWE-285 (Improper Authorization), CWE-287 (Improper Authentication), and CWE-522 (Insufficiently Protected Credentials). Salesforce responded by disabling Klue's app integration globally. No patch is applicable; remediation requires OAuth token revocation, re-authorization audits, and credential lifecycle remediation within Klue's platform. The

initial vector, a legacy credential, indicates inadequate credential rotation and offboarding hygiene, not a zero-day or product vulnerability.

Action Checklist

1. Step 1: Containment, Immediately audit all active OAuth tokens and connected app authorizations in your Salesforce org. Navigate to Setup > Integrations > Connected Apps > Manage Connected Apps and revoke any Klue-related tokens. Confirm with your Salesforce admin that Salesforce has already disabled the Klue integration at the platform level; do not assume revocation is complete without independent verification in your own org.
2. Step 2: Detection, Review Salesforce event logs for anomalous API access patterns originating from Klue's OAuth client IDs, particularly bulk data queries, export events, or access outside normal business hours. Enable and query the Salesforce Event Monitoring logs (if licensed) for EventType=ApiTotalUsage and ConnectedApp=Klue. Cross-reference with AU-6 (Audit Record Review, Analysis, and Reporting) procedures. Alert on any access events attributed to Klue tokens after the breach disclosure date.
3. Step 3: Eradication, Revoke all Klue-issued OAuth tokens across every connected Salesforce environment. Remove the Klue connected app from Salesforce Setup > Integrations > Connected Apps > Manage Connected Apps. Conduct a full review of all third-party SaaS integrations holding active OAuth grants to Salesforce and revoke any that are unused, legacy, or unverified. Apply CIS 6.2 (Establish an Access Revoking Process) to ensure OAuth grants are subject to the same deprovisioning controls as user accounts.
4. Step 4: Recovery, After token revocation, re-establish only required Salesforce integrations using freshly issued, minimally scoped OAuth tokens with explicit field-level and object-level permission restrictions. Validate that no unauthorized accounts, forwarding rules, or scheduled exports were created in affected Salesforce orgs during the access window. Monitor Salesforce audit logs continuously for 30 days post-remediation for residual unauthorized activity per AU-6.
5. Step 5: Post-Incident, This incident exposes three control gaps: (1) third-party OAuth grants are not subject to periodic review or rotation, implement D3-CRO (Credential Rotation) for all OAuth tokens held by SaaS integrations; (2) legacy credentials in vendor environments create persistent supply chain risk, require vendors to attest to credential lifecycle management under AC-2 (Account Management) as part of third-party risk assessments; (3) OAuth scopes were likely broader than necessary, enforce least-privilege OAuth scoping per AC-6 (Least Privilege) for all future integrations and audit existing grants against business justification.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if Salesforce Event Monitoring logs confirm ReportExport or BulkApiResult events under the Klue connected app during the breach window, if the affected Salesforce org contains PII, PHI, or regulated financial data triggering GDPR/CCPA/HIPAA breach notification obligations, or if the organization lacks the Event Monitoring license needed to determine exfiltration scope and must engage Salesforce support or a DFIR retainer to retrieve telemetry.

Recovery Notes	After revoking Klue's OAuth tokens and removing the connected app, verify org integrity by auditing all user accounts, Apex triggers, workflow rules, and scheduled data export jobs created during the Icarus access window — these represent persistence mechanisms beyond the token itself. Re-issue only minimally scoped OAuth grants for verified replacement integrations and enforce field-level security restrictions on any new connected app. Maintain continuous Salesforce Setup Audit Trail and Event Monitoring review for 30 days post-remediation, specifically alerting on new ConnectedApp authorizations, bulk API calls exceeding 5,000 rows, and ReportExport events from non-human service accounts.
Forensic Artifacts	Salesforce Event Monitoring logs (EventLogFile object) — ApiTotalUsage, ReportExport, and BulkApiResult event types filtered on ConnectedApp=Klue, preserving CLIENT_IP, USER_ID_DERIVED, ROWS_PROCESSED, and timestamp fields that document the scope and timing of Icarus data exfiltration | Salesforce Setup Audit Trail (180-day retention) — filtered for configuration changes made under the Klue connected app identity, including any Workflow Rules, Apex triggers, or scheduled export jobs created during the access window that Icarus may have planted as persistence mechanisms | Salesforce Login History (Setup > Login History) — OAuth-sourced login events tied to Klue's client_id, capturing source IPs, timestamps, and API versions used, which may allow correlation against Icarus infrastructure indicators if the threat actor's IP ranges become available via threat intelligence | Klue-side incident disclosure artifacts — any IOCs, Klue's legacy credential identifier, and the OAuth client_id values published or shared by Klue during breach notification, used to scope the exact token identities that require revocation across all connected Salesforce orgs | Salesforce Connected Apps OAuth Usage export (CSV) — snapshot of all active connected app grants at time of discovery, capturing consumer keys, last-used dates, and granted scopes for Klue and any other third-party SaaS integrations, serving as baseline evidence for the scope of the third-party OAuth exposure

Per-Action IR Details

Step 1: Containment — Immediately audit all active OAuth tokens and connected app authorizations in your Salesforce org. Navigate to Setup > Connected Apps OAuth Usage and revoke any Klue-related tokens. Confirm with your Salesforce admin that Salesforce has already disabled the Klue integration at the platform level; do not assume revocation is complete without independent verification in your own org.

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: Without a SIEM, export the Salesforce Connected Apps OAuth Usage report via Setup > Connected Apps OAuth Usage, then export as CSV. Use a two-person review: one runs `sf org list auth` via Salesforce CLI to enumerate all authenticated sessions, the second cross-references the Klue client_id against the org's OAuth token table at /services/oauth2/token endpoints captured in prior access logs. Document each revoked token with timestamp.

Evidence: Before revoking any tokens, capture a full snapshot of the Salesforce Connected Apps OAuth Usage page (screenshot and CSV export) preserving Klue's client_id, last-used timestamp, and granted scopes. Pull Salesforce Event Monitoring logs for the preceding 90 days filtered on ConnectedApp=Klue — this captures the active session window Icarus used. Export Salesforce Login History (Setup > Login History) filtered to OAuth source IPs associated with Klue before any revocation action destroys the live session state.

Step 2: Detection — Review Salesforce event logs for anomalous API access patterns originating from Klue's OAuth client IDs, particularly bulk data queries, export events, or access outside normal business hours. Enable and query the Salesforce Event Monitoring logs (if licensed) for EventType=ApiTotalUsage and ConnectedApp=Klue. Cross-reference with AU-6 (Audit Record Review, Analysis, and Reporting) procedures.

Alert on any access events attributed to Klue tokens after the breach disclosure date.

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-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a licensed Event Monitoring add-on, use Salesforce's free Setup Audit Trail (Setup > View Setup Audit Trail, 180-day retention) filtered for changes made under the Klue connected app identity. Run a SOQL query via Salesforce Workbench (workbench.developerforce.com) against the EventLogFile object: `SELECT Id, EventType, LogDate FROM EventLogFile WHERE EventType='ApiTotalUsage' ORDER BY LogDate DESC` — download resulting CSVs and parse with Python pandas, grouping by USER_ID_DERIVED and filtering on off-hours timestamps (outside 08:00–18:00 local org time). Flag any session with ROW_COUNT > 5000 in a single API call as a bulk exfiltration indicator.

Evidence: Preserve Salesforce Event Monitoring log files (ApiTotalUsage, ReportExport, and BulkApiResult event types) for the entire period Klue's OAuth token was active — not just post-disclosure. Specifically capture ReportExport events showing REPORT_ID, ROWS_PROCESSED, and CLIENT_IP fields, which would reveal which Salesforce reports Icarus queried during the exfiltration window. Retain the raw EventLogFile records before any log rotation or 30-day free-tier purge; export to an immutable S3 bucket or equivalent immediately.

Step 3: Eradication — Revoke all Klue-issued OAuth tokens across every connected Salesforce environment. Remove the Klue connected app from Salesforce Setup > Connected Apps. Conduct a full review of all third-party SaaS integrations holding active OAuth grants to Salesforce and revoke any that are unused, legacy, or unverified. Apply CIS 6.2 (Establish an Access Revoking Process) to ensure OAuth grants are subject to the same deprovisioning controls as user accounts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 6.2 (Establish an Access Revoking Process), CIS 5.3 (Disable Dormant Accounts)

Compensating: Without an identity governance platform, enumerate all connected app OAuth grants using Salesforce CLI: `sf org display --verbose` across each org, then run a SOQL query via Workbench — `SELECT Id, AppName, LastUsedDate, UserId FROM ConnectedApplication` — to identify any grant with LastUsedDate older than 90 days. Manually delete each stale grant via Setup > Connected Apps > OAuth Usage > Revoke. Document each removed integration with business justification for future audit evidence.

Evidence: Before removing the Klue connected app entry from Salesforce Setup, export the full Connected App configuration record including consumer key, granted OAuth scopes, callback URLs, and IP relaxation settings — these fields document the exact privilege surface Icarus exploited. Capture the Setup Audit Trail entries showing when the Klue app was originally authorized and by which Salesforce admin, preserving the chain of custody. This evidence is consumed by the deletion action; it cannot be recovered from the app record post-removal.

Step 4: Recovery — After token revocation, re-establish only required Salesforce integrations using freshly issued, minimally scoped OAuth tokens with explicit field-level and object-level permission restrictions. Validate that no unauthorized accounts, forwarding rules, or scheduled exports were created in affected Salesforce orgs during the access window. Monitor Salesforce audit logs continuously for 30 days post-remediation for residual unauthorized activity per AU-6.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.1 (Establish an Access Granting Process)

Compensating: Without automated access certification tooling, manually audit Salesforce user accounts created or modified during the Klue access window by querying Setup > Users filtered by CreatedDate spanning the breach period. Run SOQL: `SELECT Id, Username, CreatedDate, LastLoginDate, IsActive FROM User WHERE CreatedDate

>= LAST_90_DAYS` and flag any account not traceable to an approved provisioning ticket. Check scheduled Salesforce Data Export jobs (Setup > Data Export) for any job created during the access window that lacks a business owner — these represent persistent exfiltration mechanisms Icarus may have left behind.

Evidence: Before re-issuing new OAuth grants, verify no persistence mechanisms remain by querying Salesforce for unauthorized Workflow Rules, Process Builder flows, or Apex triggers that could exfiltrate data to external endpoints — run `SELECT Id, Name, CreatedDate, CreatedById FROM WorkflowRule WHERE CreatedDate >= [breach start date]` and cross-reference CreatedById against known admin accounts. Export the Salesforce Setup Audit Trail covering the entire Icarus access window to preserve the record of any configuration changes made under the Klue token identity before the 180-day retention expires.

Step 5: Post-Incident — This incident exposes three control gaps: (1) third-party OAuth grants are not subject to periodic review or rotation — implement D3-CRO (Credential Rotation) for all OAuth tokens held by SaaS integrations; (2) legacy credentials in vendor environments create persistent supply chain risk — require vendors to attest to credential lifecycle management under AC-2 (Account Management) as part of third-party risk assessments; (3) OAuth scopes were likely broader than necessary — enforce least-privilege OAuth scoping per AC-6 (Least Privilege) for all future integrations and audit existing grants against business justification.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without a SaaS security posture management (SSPM) tool, build a manual OAuth grant registry in a spreadsheet tracking: vendor name, Salesforce connected app consumer key, granted scopes, data objects accessible, business owner, last-reviewed date, and next-review date. Schedule a quarterly calendar reminder to re-run the SOQL enumeration query from Step 3 against all Salesforce orgs. For vendor attestation, add a SaaS vendor questionnaire item to your third-party risk assessment template requiring vendors to describe their credential rotation policy and attest to maximum credential age for any integration account accessing your Salesforce environment.

Evidence: Preserve the full incident timeline — from Klue's legacy credential compromise through Icarus token theft to downstream Salesforce exfiltration — as a structured lessons-learned artifact documenting the trust-chain failure: a single stale credential in a vendor's environment propagated to credential-less access across multiple customer orgs. Retain all exported Salesforce Event Monitoring logs, Setup Audit Trail exports, and Connected App configuration snapshots as post-incident evidence for regulatory breach notification analysis, given that confirmed exfiltration at named organizations (Recorded Future, Tanium, Jamf, Sprout Social, Gong, Insurity) may trigger GDPR, CCPA, or state-level notification obligations depending on the data types extracted.

Detection Guidance

Query Salesforce Event Monitoring logs for API calls attributed to the Klue connected app client ID, focusing on bulk object queries (SOQL against Account, Contact, Opportunity, Lead objects), data export events, and any access timestamped outside your organization's normal business hours. If you do not have Event Monitoring licensed, check Setup > Login History filtered by OAuth-based logins and cross-reference connected app names. Look for access patterns consistent with T1114 (Email Collection) and T1528 (Steal Application Access Token): large record-count responses, sequential object enumeration, or API calls from IP ranges not associated with Klue's documented infrastructure. Behavioral indicator: high-volume read operations on CRM objects with no corresponding user-initiated workflow. Per AU-3, ensure audit records capture what data was accessed, when, from which source IP, and under which OAuth grant, gaps in any of these fields indicate a logging control deficiency that must be corrected before the investigation can be closed.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://thehackernews.com/2026/06/salesforce-disables-klue-app.html`	The Hacker News coverage of Salesforce disabling Klue app integration following OAuth token abuse	MEDIUM
URL	`https://www.bleepingcomputer.com/news/security/klue-oauth-breach-victim-list-grows-as-icarus-hackers-claim-attack/`	BleepingComputer coverage of victim list expansion and Icarus group claim of responsibility	MEDIUM
URL	`https://www.recordedfuture.com/blog/klue-security-incident`	Recorded Future's official disclosure of its own exposure via the Klue integration breach	MEDIUM
URL	`https://www.tanium.com/blog/security-update-taniums-response-to-the-klue-breach-that-allowed-data-exfiltration-from-salesforce/`	Tanium's official security update disclosing Salesforce data exfiltration via the Klue breach	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1078.004** — Cloud Accounts
- **T1114** — Email Collection
- **T1528** — Steal Application Access Token
- **T1550.001** — Application Access Token
- **T1078** — Valid Accounts
- **T1199** — Trusted Relationship

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

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

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

- **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
T1078.004	Cloud Accounts	Defense-Evasion
T1114	Email Collection	Collection
T1528	Steal Application Access Token	Credential-Access
T1550.001	Application Access Token	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
Salesforce Disables Klue App Integration After OAuth Token Abuse ...	https://thehackernews.com/2026/06/salesforce-disables-klue-app.html	T3
Klue OAuth breach victim list grows as Icarus hackers claim attack	https://www.bleepingcomputer.com/news/security/klue-oauth-breach-vi...	T3
The Klue Security Incident and Its Impact on Recorded Future	https://www.recordedfuture.com/blog/klue-security-incident	T3
International Cyber Digest	https://x.com/IntCyberDigest/status/2067978461671506252	T3
Security Update: Tanium's Response to the Klue Breach that ...	https://www.tanium.com/blog/security-update-taniums-response-to-the...	T3

Generated 2026-06-22 06:22 UTC by TJS Security Command Center