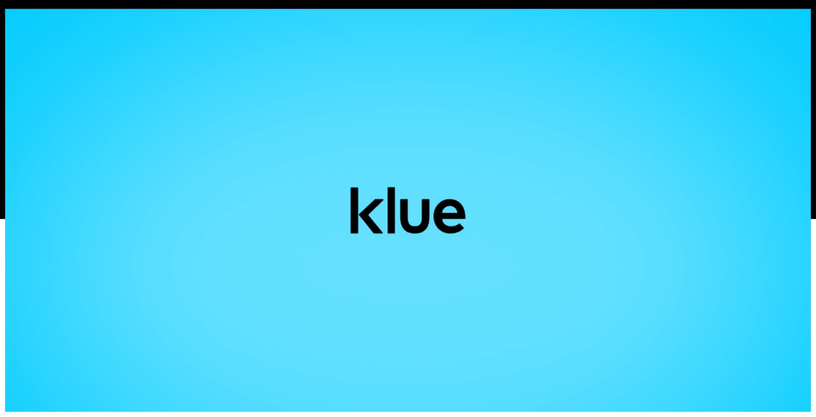
ARTICLE

An Update on the Recent Klue Security Incident

By Jason Smith 3 min read
June 18, 2026



SHARE THIS POST

Read the Completed CrowdStrike Investigation Summary (July 1, 2026)

This week we have been investigating a security incident affecting Klue, our customers, and our integration partners. I want to be direct with you about what happened, where our investigation stands, and how we're moving forward while our integrations are temporarily disconnected.

Everything we do starts with people – our customers, our team, and the trust that holds it all together. That's why we've openly and candidly shared daily updates with customers through our support center, direct emails and 1:1 meetings. This post is for the broader community. As we work with our partners to understand the scope and impact of this incident, we are committed to communicating what happened and how we can protect one another and the broader ecosystem.

What Happened

On June 12, we identified unauthorized activity affecting a portion of Klue's integration infrastructure. Since then, we've been working alongside trusted cybersecurity experts to understand what happened, support our customers, and restore the connections you rely on. Our investigation determined that an attacker gained access through a compromised legacy credential associated with an integration service. The attacker used that access to obtain OAuth tokens used to connect Klue with certain third-party platforms, including Salesforce, and subsequently accessed data within a number of connected customer environments. Based on our investigation to date, the incident was limited to the affected third-party platforms, and there is no evidence that customer content stored within the Klue platform was impacted. We recognize that customers rely on Klue to securely connect to their systems, and we understand the seriousness of that responsibility.

Our Response

We immediately took steps to contain the activity, including revoking affected credentials and tokens, removing unauthorized code, disabling potentially impacted integrations, launching a comprehensive investigation, and notifying law enforcement. Since identifying the incident, we have been communicating directly with affected customers, sharing investigative findings and supporting their response efforts. Specific remediation guidance has been shared directly with affected customers. To support our investigation and validate our response, we engaged CrowdStrike. We are also conducting a thorough review of our security controls, credential management practices, monitoring capabilities, and deployment processes. Based on those findings, we will implement additional safeguards where needed to further strengthen our environment. Customers with questions can contact their Customer Success Manager directly or reach out to our Security Team at security@klue.com.

Our Commitment

Trust is earned through actions, and our commitment is to support our customers, be transparent about what we learn, and to emerge from this incident stronger. We are committed to protecting your data, and we know an incident like this tests that commitment. We also want to be clear about what this was: a deliberate criminal act. The reality of connected software is that a single compromise can ripple across many organizations. The only way we beat these threats is by working together and sharing information and strategies. That context doesn't change our accountability. As this story unfolds, we will continue to share relevant details with our customers and help build a more resilient and secure community together.

Jason Smith
CEO, Klue

Browse by type

ARTICLES COURSES PRODUCT GUIDES REPORTS TEMPLATES

Want to see Klue in action?

Let's do it. Tell us a bit about yourself and we'll set up a time to wow you.

GET A DEMO