Chainalysis Says Attack Exposed All Users' Credentials and Tokens



Chainalysis says its investigation into an agentic cyber attack found that names, usernames, password hashes and live tokens of all users were exposed. Access to Reactor and Data Solutions was removed during the investigation.

- The investigation into an agentic cyber attack on Chainalysis systems is ongoing.
- Exposed data covers all users: names, usernames, password hashes and live tokens.
- Chainalysis removed access to Reactor and Data Solutions while investigating.
- The company states it has no evidence so far that investigations data was accessed.

What was disclosed

Blockchain analysis firm Chainalysis has said that its continuing investigation into an agentic cyber attack on its systems found that the exposure extends to all users. The affected data includes names, usernames, password hashes and live tokens.

While investigating, the company removed access to two services, Reactor and Data Solutions. It also said it still has no evidence that any investigations data has been accessed. The source does not give further detail on the attack, its timing or how many users are involved.

Why it matters

Live tokens are the most time-sensitive element. A valid token may allow access without a password, so changing passwords alone may not close the exposure. Password hashes also carry risk if passwords are weak or reused elsewhere.

Institutions in the Kingdom that use Chainalysis products, for example in financial crime or transaction monitoring work, should treat this as a third-party exposure and confirm their own position with the vendor rather than wait for further public detail.

Recommended approach

The steps below are precautionary and fit within normal third-party and identity incident handling. Adjust scope once the vendor confirms which accounts and services affect your organisation.

What to do now

1. Confirm with Chainalysis whether your organisation's accounts and services are affected.
2. Revoke and reissue active tokens, sessions and API keys tied to Chainalysis services.
3. Reset passwords for affected accounts and for any other systems where the same passwords were used.
4. Enforce multi-factor authentication on vendor portals and review recent login activity for anomalies.
5. Record the event in your third-party risk register and assess whether any internal notification duties apply.