Chainstack discloses breach of production systems, with customer data and password hashes exposed



Blockchain infrastructure provider Chainstack disclosed that an unauthorized party accessed parts of its infrastructure. It links the incident to a large AI-powered attack campaign that surfaced last week.

- Chainstack disclosed on Tuesday that an external attacker gained unauthorized access to part of its infrastructure.
- The headline reports that customer data and password hashes were exposed.
- The incident is assessed as part of a large-scale, AI-powered attack campaign that emerged last week.
- The excerpt available does not give the full scope, timeline or technical details.

Chainstack, a blockchain infrastructure provider, has disclosed that it was targeted in a cyber attack in which an unauthorized party gained access to some parts of its infrastructure.

What has been reported

According to the report, the company says an external attacker accessed part of its systems. The headline states that production systems were affected and that customer data and password hashes were exposed. The incident is assessed to belong to a large-scale attack campaign that uses artificial intelligence and that came to light last week.

The portion of the source available to us is brief. It does not set out how many customers are affected, which data fields were involved, how access was obtained or how long it lasted. We therefore avoid drawing conclusions beyond what the company has stated.

Why it matters for regulated institutions

Institutions in the Kingdom that use blockchain or node infrastructure services, or that rely on third-party platforms holding credentials, should treat this as a prompt to check their own exposure. Exposed password hashes are not the same as exposed passwords, but they can still raise risk if credentials are weak or reused elsewhere.

The practical step is to confirm whether Chainstack is in your supplier inventory, read the company's own notice directly, and decide on precautionary measures based on what it says. Where personal data may be involved, your legal and privacy teams should assess notification duties under the PDPL.

What to do now

1. Check whether Chainstack is used by your organization or by any critical supplier, and identify the accounts and API keys involved.
2. Read Chainstack's official notice and follow its guidance on credential resets and key rotation.
3. Rotate passwords and API keys linked to the service, and enforce multi-factor authentication where available.
4. Ensure the same passwords are not reused on other systems, and reset them if they are.
5. Monitor logs for unusual logins or API activity tied to the affected accounts.
6. If personal data may be affected, have legal and privacy teams assess PDPL notification obligations.