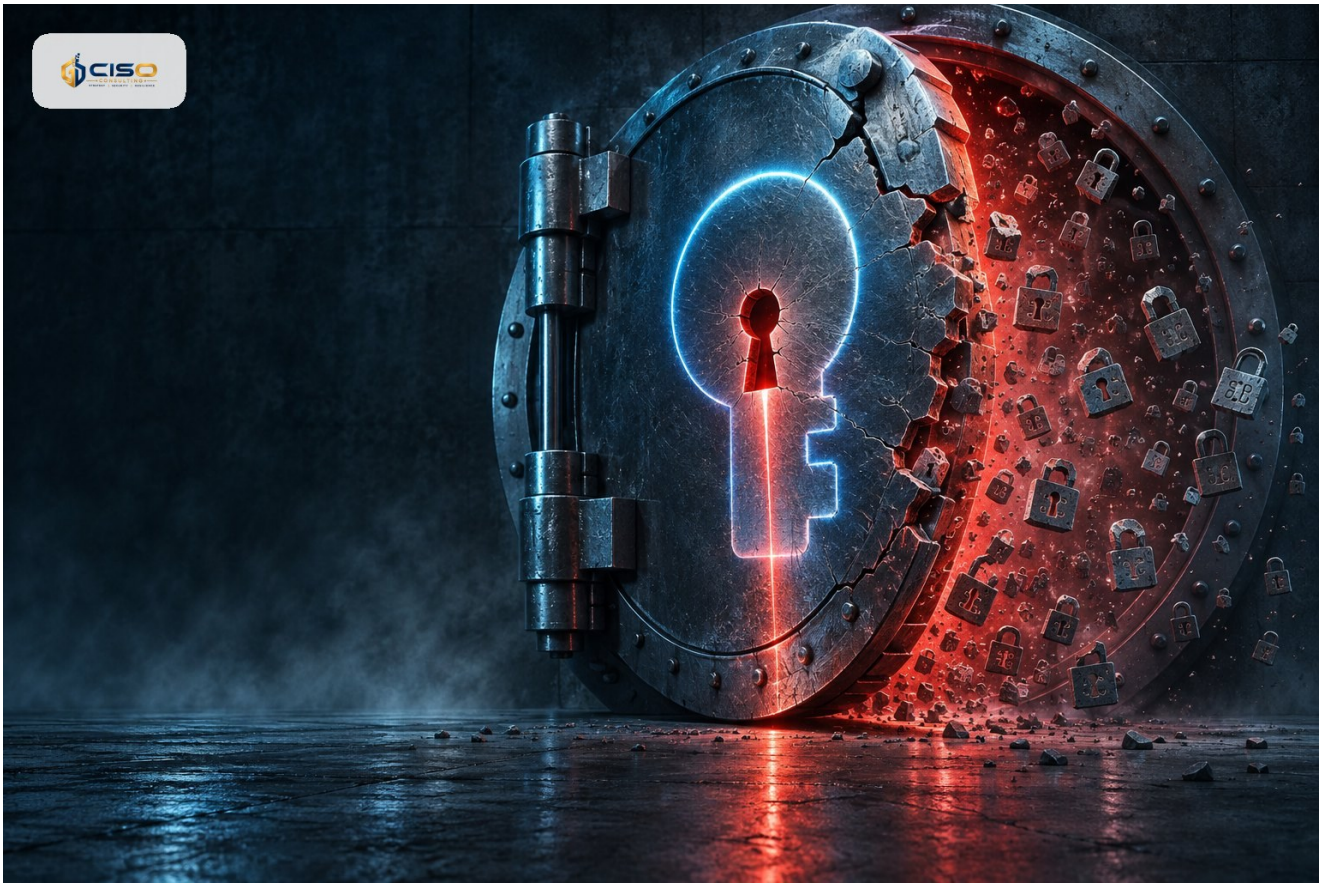
mSecure password manager breach: customers told to reset credentials



mSeven Software has told current and former mSecure customers to change passwords, reset two-factor authentication and remove passkeys after a cyberattack that reportedly exposed an encrypted customer database.

- mSeven Software, the maker of the mSecure password manager, is warning customers after a cyberattack.
- The attack reportedly exposed an encrypted customer database.
- Both current and former customers are advised to act.
- Recommended steps: change passwords, reset two-factor authentication and remove passkeys.

What was reported

mSeven Software, the company behind the mSecure password manager, has warned current and former customers to take protective steps following a cyberattack. According to reports, the incident exposed an encrypted customer database.

The company's guidance is to change passwords, reset two-factor authentication and remove passkeys. The advice applies to former customers as well as active ones, so people who no longer use the product may still need to act.

What the source does not say

The available text does not set out further technical detail, such as the scope of the data involved or the timeline of the incident. Organisations should avoid assuming more than has been stated and should follow the vendor's own notices as they are updated.

Why it matters for regulated institutions

Password managers hold the credentials that protect other systems. Even when stored data is encrypted, a precautionary reset limits the window in which exposed material could be useful to an attacker. Employees may also use personal or legacy password manager accounts for work logins, which security teams often cannot see.

A calm, structured response is sensible: find out whether the product is in use, ask staff to complete the vendor's recommended resets, and prioritise accounts with privileged or remote access.

What to do now

1. Check whether mSecure is used by staff, including personal accounts used for work logins.
2. Ask current and former mSecure users to change passwords, reset two-factor authentication and remove passkeys as the vendor advises.
3. Prioritise resets for privileged, remote-access and critical business accounts.
4. Review sign-in logs for unusual activity on accounts whose credentials were stored in mSecure.
5. Monitor mSeven Software's notices and update internal guidance if new details are released.