pCloud Pass confirms cyber attack after users report unknown devices on accounts



pCloud Pass, a password manager from a Swiss company, confirmed it was targeted by a cyber attack that its team says was contained. Users had reported unknown devices linked to their accounts.

- pCloud Pass is a cross-platform password manager from a Swiss company.
- Users reported unknown devices connected to their accounts, including in posts on Reddit.
- The company confirmed an attack and said its team promptly contained it.
- It said a small number of users had email addresses affected; the source text is cut off after that point.
- The source does not state the scope of exposure beyond this, nor any cause.

What was reported

The Swiss company behind pCloud Pass has acknowledged that its cross-platform password manager was the target of a cyber attack. The acknowledgement followed posts on Reddit in which users said they had seen unknown devices connected to their accounts.

In its response, the company said the attack was promptly contained by its team. It also said that a small number of users had their email addresses affected. The source text ends there, so further detail on what else was exposed, how the attackers got in, or how many accounts were involved is not available.

What this means for institutions

A password manager holds credentials for many other systems, so any incident involving one deserves attention even when the vendor describes it as contained. The reported symptom, unfamiliar devices appearing on accounts, is something users and security teams can check directly.

Organisations should avoid drawing conclusions beyond what the vendor has said. The sensible approach is to establish whether staff use the product, confirm account state, and follow any further notices from the vendor.

Recommended approach

Treat this as a precautionary review rather than an emergency. Confirm exposure first, then tighten account hygiene where pCloud Pass is in use, and keep records of the checks in case regulators or auditors ask.

What to do now

1. Check whether staff or business units use pCloud Pass, including personal use for work credentials.
2. Ask users to review the list of connected devices in their pCloud Pass accounts and remove any they do not recognise.
3. Advise affected users to change their master password and enable multi-factor authentication if available.
4. Warn staff that email addresses may be used for phishing and to report suspicious messages.
5. Monitor vendor notices and, if personal data of customers or staff is confirmed affected, assess notification duties under PDPL.
6. Document the review and outcome for audit and third-party risk records.