pCloud confirms attack on its Pass password manager; vault exposure not ruled out



pCloud says a contained attack on pCloud Pass exposed a small number of email addresses and led to login attempts. It says stored data stays encrypted, but has not said whether encrypted vaults were accessed.

- Users received alerts about a new device named "pd" connecting to their pCloud Pass accounts, some with 2FA enabled.
- pCloud says the attack was contained, limited to the password manager, and did not affect cloud storage.
- The company says a small number of email addresses were exposed and login attempts were made.
- pCloud says vault data is encrypted on user devices and needs the master password, but it has not

> said whether encrypted vaults were accessed or stolen.
>
> - Alert emails reportedly linked to a hostname that appears to be a QA environment.

pCloud has confirmed that its password manager, pCloud Pass, suffered a cyberattack. The incident surfaced when customers received emails saying an unfamiliar device named "pd" had connected to their accounts. Some said they had 2FA enabled, and some saw no unknown device when they checked their account. Others who had never used the password manager also received the alerts.

What pCloud says

pCloud states that the attack was promptly contained and isolated to the password manager, with cloud storage unaffected. It says a small number of user email addresses were exposed and login attempts were made, and that the automatic notifications went to those addresses. The company says passwords, notes and other stored items were not compromised, because they are encrypted on customers' devices and can only be decrypted with the master password.

What remains unclear

pCloud did not say whether any encrypted vaults were accessed or stolen. That matters because an attacker holding encrypted vaults can attempt offline cracking, which bypasses login rate limits and 2FA. The source recalls the 2022 LastPass breach, where stolen vault backups were later linked to cryptocurrency thefts believed to involve weak or reused master passwords.

A reader also noted that the "Open settings" link in the notification pointed to a hostname that appears to be a QA environment rather than production. BleepingComputer confirmed this in a copy of the email. pCloud also warned customers about phishing and said it never asks for master passwords or recovery words by email, phone or chat.

The incident follows other password manager incidents this month, involving mSecure and 1Password, according to the source.

What to do now

1. Identify staff and business units using pCloud Pass or similar consumer password managers, and confirm whether corporate credentials are stored there.
2. Ask affected users to change their master password to a long, unique passphrase and rotate high-value credentials stored in the vault.
3. Do not rely on the pCloud statement alone: request clarification from the vendor on whether encrypted vaults were accessed.
4. Warn staff that pCloud says it never requests master passwords or recovery words, and that notification emails may be used as phishing lures; verify links before clicking.

5. Where third-party password managers are in use, review the supplier risk assessment and incident notification terms in line with NCA ECC and SAMA CSF third-party requirements.