1Password discloses breach via employee GitHub account; vaults not affected



1Password says an attacker used a compromised employee GitHub account to inject code that pulled customer account records. Vaults and their keys were not affected; phishing using the stolen data is the main risk.

- Investigation began on November 19 after signs that an employee's GitHub account was compromised.
- The attacker injected malicious code into backend services and downloaded customer account records.
- Exposed data includes names, emails, IDs, timestamps, public keys, SRP parameters and invitation or recovery tokens.
- Internal source code was stolen and the CI/CD environment was accessed, potentially exposing

> infrastructure credentials.
>
> - Only a small number of users were affected; no password or Secret Key change is required.

1Password has disclosed a security incident in which an attacker took over an employee's corporate GitHub account, reached private source code repositories and inserted malicious code into backend services. That code was used to download customer account records.

What was affected

The company states that customer password vaults and the encryption keys protecting them were not compromised. The stolen records include customer names and email addresses, account and user IDs, creation and last sign-in timestamps, public cryptographic keys, Secure Remote Password (SRP) parameters, and invitation, provisioning and account recovery tokens. The attacker also took internal source code and accessed the CI/CD environment, which could have exposed infrastructure credentials.

The tokens cannot be used alone: completing an invitation or recovery requires either SSO authentication or a code sent to the user's registered email. 1Password has lengthened that code from six digits to ten alphanumeric characters as a precaution against brute-force attempts. Affected users, described as a small number, have been notified individually.

Response and remaining risk

1Password disabled the compromised account, revoked the stolen token, restored clean versions of affected services and rotated or revoked potentially exposed credentials. Independent experts are validating the remediation, and the company reports no internal evidence of account takeovers. It is not asking customers to change passwords or Secret Keys.

The practical risk is phishing. The stolen data identifies real 1Password users, and attackers may send emails posing as the company, urging users to secure accounts, reset passwords or verify details. Users should open the website or app directly rather than follow email links, and never share passwords, Secret Keys or verification codes.

What to do now

1. Identify which business units and staff use 1Password and record it as a third-party exposure in the risk register.
2. Warn users about phishing that cites this breach, especially emails asking to secure accounts, reset passwords or verify details.
3. Tell users to reach 1Password only via its website or app, and never share passwords, Secret Keys or verification codes.
4. Have the security team flag unexpected invitation or account recovery emails and review related sign-in

activity.

5. Ask 1Password for written confirmation of impact and remediation, and check notification duties under PDPL and sector rules if personal data of your staff is involved.
6. Review your own protection of GitHub accounts and CI/CD credentials: MFA, token scope and rotation.