1Password discloses breach of customer records and source code; vaults not affected



1Password says an attacker used a compromised employee GitHub account to take customer records and source code. The company reports no evidence that encrypted vaults were accessed, and its investigation continues.

- Investigation began on November 19 after an employee's corporate GitHub account was suspected of compromise.
- Exposed records include names, email addresses, account identifiers, public keys, authentication parameters, activity times and non-secret metadata.
- The attacker also took private source code and accessed the CI/CD system, potentially exposing infrastructure credentials.
- 1Password reports no evidence that encrypted vaults were downloaded or accessed; client apps,

> browser extensions and recovery keys are unaffected.
>
> - The number of affected users and the initial access method remain unclear.

1Password, a password management and identity security company, disclosed that an attacker stole customer information and proprietary source code. The company began investigating on November 19, after an employee's corporate GitHub account was thought to be compromised.

What was affected

According to the report, the attacker used the account to deploy malicious code to backend services and extract customer records. These contain names, email addresses, account identifiers, public cryptographic keys, authentication parameters, account activity times and non-secret metadata. The attacker also obtained source code from private repositories and reached the CI/CD system, which could have exposed infrastructure credentials. Tokens from emails sent for account invitations, provisioning and recovery were taken as well. A small number of people going through provisioning or recovery at the time were notified. 1Password says these tokens cannot be used alone and it has no evidence of account hijacking.

The stolen authentication data included Secure Remote Password verifiers. The company states they cannot be used directly to authenticate, and guessing passwords would need the Secret Keys, which 1Password does not store.

Response and open questions

1Password says customer vaults and the keys protecting them were not compromised, and it has no evidence that encrypted vaults were accessed. Client applications, browser extensions and account recovery keys are not affected. The company disabled the compromised account, invalidated a stolen token, replaced potentially exposed infrastructure credentials and restored clean versions of affected services. The investigation, supported by independent experts, is ongoing.

It is still unclear how many users are affected and how the attacker first got into the GitHub account. The company says customers need not act, but should watch for phishing that exploits the news.

What to do now

1. Confirm whether your organisation uses 1Password and follow the vendor's updates as the investigation develops.
2. Warn staff and administrators about phishing emails that reference this incident, and route suspicious messages to the security team.
3. Review your own developer accounts: enforce MFA on GitHub and similar platforms and audit access to private repositories and CI/CD systems.
4. Check that CI/CD secrets and tokens can be rotated quickly, and test that process.

5. Record the incident in your third-party risk register and ask the vendor for written assurance on impact, as your NCA ECC and SAMA CSF obligations require.