# DreamHost confirms breach exposed customer FTP logins and webmail sessions



DreamHost says attackers had access to its File Manager platform for two months and stole customers' FTP/SFTP usernames and passwords. Hosting customers should rotate credentials and review access.

- DreamHost has confirmed a data breach affecting its File Manager platform.
- Attackers had access for two months.
- Stolen data includes customers' FTP/SFTP usernames and passwords.
- The headline also reports exposure of webmail sessions.
- The source text available does not provide further detail such as customer numbers.

## What happened

DreamHost has warned customers of a data breach. According to the report, attackers gained access to its File Manager platform and kept that access for two months. During that time they stole customers' FTP and SFTP usernames and passwords. The report's headline also states that webmail sessions were exposed.

## What is not yet known

The portion of the report available to us is limited. It does not give the number of affected customers, the method of intrusion, or the exact dates, so we do not speculate on them. Organisations should rely on DreamHost's own notifications for scope and remediation guidance.

## Why it matters

FTP and SFTP credentials usually grant direct write access to website files. If an institution, or a vendor acting for it, hosts a website or file transfer area with this provider, stolen credentials could allow content to be altered or files to be read. Exposed webmail sessions raise a similar concern for mailbox access.

The sensible response is calm and procedural: establish whether you use the provider, change credentials, end active sessions and check logs for activity you do not recognise. Third-party hosting, including services bought by marketing or business teams outside IT, is often missed in inventories, so this is a good moment to confirm what is actually in use.

## What to do now

1. Check whether any corporate or vendor-run site, mailbox or file transfer area is hosted with DreamHost.
2. Reset FTP/SFTP passwords for affected accounts and end active webmail sessions.
3. Review access and file-change logs for the exposure period for unfamiliar logins or modified files.
4. Do not reuse the exposed passwords elsewhere; enforce unique credentials and multi-factor authentication where offered.
5. Ask vendors in writing whether they use the provider, and update the third-party inventory and incident log.