Advisory: VSee Clinic

2026-07-20 :: Security Risk Advisors

#advisory #CVE-2026-13381 #CVE-2026-13380

Summary

SRA has identified multiple vulnerabilities in VSee Clinic that can lead to unauthorized access to and deletion of files as well as exposure of SFTP credentials.

CVE Identifiers

CVE ID	CVE Name
CVE-2026-13380	VSee Clinic and API Insecure Direct Object Reference in File API Allows Unauthorized File Access and Deletion
CVE-2026-13381	VSee Clinic and API Exposes Cleartext SFTP Credentials in Unauthenticated HTTP Responses

Vulnerability Details / Description

CVE-2026-13380: VSee Clinic and API Insecure Direct Object Reference in File API Allows Unauthorized File Access and Deletion

VSee Clinic 7.1.26 and API 1.3.0 contain an Insecure Direct Object Reference (IDOR) vulnerability in the /v1.3.0/api/files endpoint. An authenticated

attacker can manipulate the ‘remark’ request parameter to enumerate, retrieve, and delete files belonging to other users on the application server.

Severity

The CVSS base score of this vulnerability has been calculated to be 8.7 (High)

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE-2026-13381: VSee Clinic and API Exposes Cleartext SFTP Credentials in Unauthenticated HTTP Responses

VSee Clinic 7.1.26 and VSee Clinic API 1.3.0 exposes cleartext SFTP credentials in the HTTP responses of three unauthenticated endpoints. The credentials are present in these responses only when SFTP connections have been configured within the application. No authentication is required to retrieve these credentials. An unauthenticated remote attacker who observes any of these HTTP responses on an instance where SFTP is configured can obtain the credentials and use them to access the associated SFTP server.

Severity

The CVSS base score of this vulnerability has been calculated to be 9.0 (Critical)

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:N

Affected Versions and Models

VSee Clinic from 7.1.26 before 7.1.26.1. VSee Clinic API from 1.3.0 before 1.3.0.1.

VSee Clinic API’s default status is uknown for CVE-2026-13380 and unaffected for CVE-2026-13381.

MITRE CWE Weakness Enumeration

CVE-2026-13380

- CWE-201 Insertion of sensitive information into sent data
- CWE-312 Cleartext storage of sensitive information

CVE-2026-13381

- CWE-639 Authorization bypass through user-controlled key

Remediation Options

Update VSee Clinic to 7.1.26.1 or later and VSee Clinic API to 1.3.0.1 or later

Source

These vulnerabilities were discovered by Chris Jones, Drew Young, and Maguire Younes as part of research performed by Security Risk Advisors.

Timeframe

- June 16, 2026 - SRA submits vulnerability to vendor
- June 24, 2026 - Vendor releases fix
- July 20, 2026 - SRA publishes CVEs and advisory