



CVE-2026-0932: SSRF Vulnerability in M-Files Server

DESCRIPTION

Blind server-side request forgery (SSRF) vulnerability in legacy connection methods of document co-authoring features in M-Files Server before 26.3 allow an unauthenticated attacker to cause M-Files Server to send HTTP GET requests to arbitrary URLs.

AFFECTED PRODUCTS

M-Files Server before 26.3.15818.5

MORE INFORMATION

Successful exploitation can reveal the IP address of the M-Files Server handling the request, but no other sensitive details are included in the GET request originating from the server. Successful abuse of the vulnerability can have a moderate performance impact on the M-Files Server instance.

CVSS 4.0 Score: 6.9

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

CWE: CWE-918 Server-Side request forgery (SSRF)

CAPEC: CAPEC-664 Server Side Request Forgery

Internal ID: CE-2644, COLAB-103, 169133

Date issued: 2026-04-01

Credits: Sina Kheirkhah (SinSinology) of watchTowr (watchTowrcyber)

Alternate IDs: –

EXPLOITABILITY

Publicly disclosed: Yes

Exploited: No

Probability of exploitation: Low

LINKS

<https://www.cve.org/CVERecord?id=CVE-2026-0932>

HISTORY

2026-04-01 Published

© 2026 - M-Files, All Rights Reserved