CYBER ADVISORY

Thursday, May 07, 2026 **CAL-CSIC-202605-A-001**

Authentication Bypass Vulnerability in Progress Software MOVEit Automation

Unauthorized Access | Confidentiality Compromise | Remote Code Execution | Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability that targets Progress Software MOVEit Automation. CVE-2026-4670 carries a CVSS 3.1 score of 9.8.[1] Successful exploitation allows an unauthenticated attacker to gain complete unauthorized access to MOVEit Automation systems without requiring valid credentials. Additionally, successful exploitation can result in a compromise in system confidentiality of sensitive data, administrative takeover, and potential lateral movement within the target network.

CVE-2026-4670 requires no user interaction, has low attack complexity, and can be performed remotely over the network from any source. There currently is no evidence of a publicly available Proof-of-Concept, nor is there confirmed exploitation in the wild.[2]

The Cal-CSIC recommends following the vendor's guidance for remediation. Additionally, for more technical vulnerability details for CVE-2026-4670, please use this link:

https://community.progress.com/s/article/MOVEit-Automation-Critical-Security-Alert-Bulletin-April-2026-CVE-2026-4670-CVE-2026-5174

Affected Product and Version:

Products	Version
Progress Software MOVEit Automation	*<=2025.1.4* *<=2025.0.8* *<=2024.1.7*

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-4670 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-4670; accessed 01 May 2026

[2] Feedly; "CVE-2026-4670"; https://feedly.com/cve/CVE-2026-4670; accessed 01 May 2026