



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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

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

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR