CYBER ADVISORY

TLP:CLEAR
30 July 2024

Progress MOVEit File Transfer Vulnerability

CVE-2024-6576 | MOVEit | SFTP | Privilege Escalation

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability under active exploitation known as CVE-2024-6576, with a CVSS v3 score of 7.3.[1,2] The vulnerability affects Progress MOVEit Transfer versions from 2023.0.0 before 2023.0.12, from 2023.1.0 before 2023.1.7, and from 2024.0.0 before 2024.0.3.[2] Exploitation of the vulnerability could allow an attacker the ability for improper authentication that can lead to privilege escalation.[3]

MOVEit Cloud has already been upgraded to the patched version, and only owned assets are affected.[3]

The Cal-CSIC recommends immediately applying the most up to date patches.

For further information on applying the most up to date Progress MOVEit Transfer patches, please refer to MOVEit Transfer Product Security Alert Bulletin – July 2024 – (CVE-2024-6576) - Progress Community.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.

Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Vuldb; "Progress MOVEit Transfer Prior 2023.0.12/2023.1.7/2024.0.3 SFTP Module Improper Authentication" https://vuldb.com/?id.272653; accessed 30 July 2024
[2] Tenable; "CVE-2024-6576" https://www.tenable.com/cve/CVE-2024-6576; Accessed 30 July 2024
[3] Progress Community "MOVEit Transfer Product Security Alert Bulletin -July 2024 – (CVE-2024-6576)" https://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-July-2024-CVE-2024-6576; accessed 30 July 2024