Fixed Issues in 2026.0.3

Last Updated: July 24, 2026 | 1 minute read | MOVEit Transfer | Version 2026 | Documentation

This section outlines issues tracked and fixed by the MOVEit product team for the 2026.0.3 Service Pack.

Note: See the What's New section for a broader summary of features and improvements.

ID	Category	Fixed Issue
81970	WebUI, logging	Fixed issue where log export requests could return error file instead of expected error response.
101356	Audit log, database	Improved audit log handling to help ensure tamper-evident logging under error conditions.
102568	WebUI, security	Improved access controls for AS2 folder management actions.
103131	REST API, security	Improved handling for GET requests.
103491	WebUI, security	Improved validation for branding logo file uploads.
103500	REST API, security	Improved token refresh handling to prevent concurrent reuse issues.
103651	MFA, security	CVE-2026-10697: Improved authentication enforcement for legacy integration endpoint.
103654	SSO/SAML, security	Improved validation and handling for SAML federation metadata imports.
103658	Key Rotation, security	Improved internal key management service by enforcing stronger access controls on privileged operations.
103660	API, security	Improved protections for internal automation endpoint to prevent unauthorized access and reduce information exposure.
103820	Sign on, performance	Reduced performance impact of host permit queries.
103824	WebUI, permissions	Fixed issue where Group member could encounter "Not enough permissions to share" message for cases where Group has *share* permissions on folder.
103838	REST API, usability	Fixed issue where temporary users could encounter internal server error when accessing the Files endpoint.
104314	Usability, security	Cleaned/removed report output metadata not relevant to users.
104593	Ad Hoc, security	Improved protections to prevent unauthorized mailbox state changes through legacy API path.
104594	Users, security	Improved argument handling for modifying organization-level user quotas.
104595, 104596.	Groups, users, security	Improved checks to prevent unexpected or accidental modification to group admin settings.
104597	WebUI, Settings (org), security	Improved org-specific validation to prevent unexpected org-level email format settings.
104598	Groups, security	Improved access controls for group member settings across organizational boundaries.

ID	Category	Fixed Issue
104599	SFTP, WebUI, security	Enhanced SFTP authentication handling to prevent unauthorized key submission and reduce unnecessary administrative notifications.
104600	Ad Hoc, security	Improved Ad Hoc component to prevent recipient information exposure.
104601	Settings (org), security	Improved access control enforcement to prevent unauthorized cross-organization configuration changes.
104675	WebUI, user auth security	Improved session security for account sign-in.
104748	WebUI, security	CVE-2026-15966: Implemented security hardening to protect authenticated sessions against unintended cross-origin resource sharing.
104768	SMTP, security	Improved SMTP transport security to prevent unintended fallback behavior during encrypted mail delivery.
104806	SSO/SAML, security	Improved SAML assertion validation to better enforce protocol compliance and strengthen authentication security.
104809	Folders, security	Improved folder copy permission enforcement to prevent unauthorized file placement in restricted locations.
104829	Downloads, security	Improved the security of token-based downloads to better protect against unauthorized access attempts.
105139	LDAP, stability	fixed issue that could cause intermittent IIS worker process crashes during LDAP/Active Directory authentication and synchronization.
105143	Audit log, security	Improved authorization checks on audit log detail access to better protect sensitive organizational activity data.
105161	Reports, security	Improved protections for session handling and reporting access.
105187	REST API, security	CVE-2026-15967: Improved token refresh checks to better enforce current account access policies.
105235	WebUI, security	Updated third-party JavaScript dependency (axios).
105249	Ad Hoc, security	Improved guest access protections to prevent unauthorized exposure of package information.
105255	Network rules, security.	Improved hostname validation to strengthen access controls and prevent allowlist bypass scenarios.
105270	WebUI, reporting	fixed issue that could cause the Package Aging report to fail with errors.
105427	FTPS, HTTPS, security	Updated third-party library (OpenSSL).
105535	Network rules, security	Improved validation of client IP addresses to improve access control for trusted proxies.
105547	WebUI, security	CVE-2026-15968: Improved input handling in the Find File page to address potential cross-site scripting issue.
105615	Ad hoc, security	Improved input handling on the guest reply compose page.
105616	SSO, security	Improved input handling on administrative IdP configuration page.
105715	Stability, WebUI	Improved stability and resilience in token revocation processing to prevent service interruptions.
105772	Database, MySQL	Updated MySQL to the latest supported version.
106002	SSO, security	Improved authentication request handling to minimize unauthenticated traffic.

ID	Category	Fixed Issue
106053	SSO/SAML, security	Addressed authentication issue to improve tenant isolation for SAML sign-in.
106056	REST API, security	Improved token request handling for better service availability when experiencing abnormal request patterns.
106069, 106070	UI, SSO, security	Improved input handling for better service availability.
106163	Database, performance	Improved database query efficiency for file operations.
107626	Downloads, security	Improved download argument parsing.