Cleo LexiCom®

# Release Notes

## Version 5.8

February 2025

RESTRICTED RIGHTS
Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (C)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227 - 7013.

**Cleo**
4949 Harrison Avenue, Suite 200
Rockford, IL 61108 USA
Phone: +1.815.654.8110
Fax: +1.815.654.8294
Email: sales@cleo.com
www.cleo.com

**Support:** 1.815.282.7894, 1.866.444.2536 (US only), 02038653439 (UK), or support@cleo.com

Cleo reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications and shall not be responsible for any loss, cost or damage, including consequential damage, caused by reliance on these materials.

# Contents

# Cleo LexiCom 5.8 Release Notes

Cleo LexiCom software provides you with a wide variety and combination of file transfer capabilities that allow you to initiate transfers, control your transfers and environment, monitor your file transfer activities, and take actions as appropriate based on your file transfer activities.

Cleo VersaLex is the platform that powers the Cleo family of Secure Data Integration (SDI) products—The Cleo LexiCom® product is a desktop-based client solution for communication with major trading networks. The Cleo VLTrader® product is a server-level solution designed to meet the needs of mid-enterprise organizations. The Cleo Harmony® product is tailored for large enterprise needs. Enterprise capabilities include system monitoring, enhanced business-level dashboards, VLTracker, SNMP traps, dynamic blacklisting, and whitelisting.

## Cleo Technical Support

Standard Cleo Technical Support is available from 7am - 7pm CST, Monday through Friday. Support availability might differ depending on your support package.

Training and a support subscription are required to work with a Cleo technical support analyst for all products, except Cleo LexiCom.

When contacting the Cleo support team, have your contact information, the name of product you are calling about, and your serial number, if available. During the support process we may request additional information (for example, a support bundle) that will vary depending on the type of request or issue.

Requests are handled on a callback basis in the order they are received. The Cleo support answering service or web form will collect your information and your request will be placed in our callback queue.

To contact Cleo Technical Support:

- Use the request form at: https://support.cleo.com/hc/en-us.
- Call us:
  - 1-815-282-7894
  - US (toll free): 1-866-444-CLEO(2536)
  - UK: 02038653439

# What's new in version 5.8

### General Enhancements

- **New REST API-based import for P12 certificates** – Enhanced endpoint now allows importing certificates.
- **New three-level support for nested ExecuteOn commands** – Commands are now supported up to three levels.
- **New Advanced Users property for Archive Nested Subdirectories** – Archive file transfers to the user and system sent/received boxes.
- **Enhanced change HTTP status code return** – Ability to control the status return code when basic authentication is disabled
- **Enhanced report generation** – Go beyond the UI grid to access file path transfer information

### Security Updates and Enhancements

- Upgraded to the latest version of log4j v2
- New SFTP algorithms and MQ SSL cipher specs
- New Admin-user level configuration to control accessibility to host visibility
- Enable Explicit AUTH Required setting for FTP
- Ensure paths in filenames on incoming requests are ignored for AS2, ebMS, RNIF, and SMTP protocols that do not support paths
- Removed the default OSGi HTTP listening port 8181

### Additional Enhancements and Fixes

- New support for MySQL 8
- Enhanced ability to execute post processing commands after a file is written
- Enhanced ebMS to modify the format of the Content-Id header and new advanced property setting
- Enhanced Message Queuing support for MQ SSL cipher specs
- Enhanced ebMS (ebMXL) configuration and advanced property settings with new Allow Incoming Request With Missing Role Element property.
- Enhanced HTTP with new Save Error Response Content On Put Plus Get advanced property setting
- Updated support for multiple SFTP client and server-side algorithms.
- Updated outbound AS4 signed messages with multiple attachments now orders digest messages the same as the attachments.
- Improved performance of SSH FTP directory listings for Linux
- Improved performance of SMB connector
- Improved S3 UI performance on startup

# Upgrading to version 5.8

When upgrading to Cleo LexiCom version 5.8, Cleo recommends the following:

- Back up your configuration using the **Export** functionality. In the Web UI, go to **Administration > System > Export**. In the native UI, go to **File > Export**. Performing an **Export** will save your data in a format that you can import using the Cleo LexiCom **Import** functionality should the need arise.
- Make sure your system meets the system requirements for Cleo LexiCom version 5.8, as it requires greater resources than earlier versions. All new installs must be 64-bit. Visit Cleo LexiCom 5.8 System Requirements to view the System Requirements for your product.
- Run the Cleo LexiCom 5.8 installer to perform an in-place upgrade. Your data and configuration remain intact from the previous version of the Cleo LexiCom software.

# Update history

The following sections contain descriptions of issues fixed in Version 5.8:

## Fixed issues in version 5.8

### Security - Framework

- VersaLex now ensures that any paths in filenames on incoming requests are ignored for protocols that do not support paths, including AS2, ebMS, RNIF, and SMTP.
- For the main VersaLex process, upgraded log4j v1 to the latest version of log4j v2.

### Enhancements - Framework

- Cleo LexiCom only: LexiCom now supports running natively on IBM iSeries (AS/400) V7R4 (with secondary Windows 7-based computer to run the user interface).
- Added a new property called "Accessing raw payload from transfer reports requires Host permissions" to Administrator User configuration. Setting this property to "false" allows users with the ability to view transfer reports (but without the ability to view hosts) to view or email raw payload. By default, this is set to "true" to replicate current functionality.
- When sending bundled Database Payload, added the ability for each file to use additional properties only when explicitly set in the VLOutgoingProperties table. All other settings use the defaults from the host, mailbox, or action. To enable this, set 'Clear.Set.Properties' to 'True' in the VLOutgoingProperties table for each file.
- Added the ability to change the HTTP status code returned when 'Disable Basic Access Authentication for REST API Requests' is turned on.
- Nested ExecuteOn... commands are now supported up to three levels. An example would be an ExecuteOnFail from a failure result of an ExeucteOnCheckConditionsMet (this would be two levels).
- The Generate Report option in the admin web UI Transfers page would previously include only the information viewable from the UI grid. Now all available transfer information, such as file path, is included in the generated report. Also, a report generated from classic mode specifically now includes the file path if it is enabled in the user's group.
- Added the ability to import a P12 certificate through the REST API.
- Improved performance renaming/moving files within the same connector.

### Enhancements - HTTP

- Added a new HTTP 'Save Error Response Content On Put Plus Get' advanced property, which when set on causes the response content from a PUT+GET command request to be saved to the inbox even on error responses.

### Enhancements - SSH FTP

- Added an option to SSHFTP Client host named 'Ignore STAT Errors' which will ignore any FXP_STAT errors when opening a directory.
- Added system options for limiting client-side SSH FTP cipher, key exchange, mac, and public key algorithms for all client connections. Go to Administration>System>Other in the admin web UI and filter on Protocols to configure regular expressions for each algorithm.
- All negotiated algorithms are now logged at the beginning of each SFTP client and server session.

- Added support for the following SFTP algorithms: Public Key: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, Key Exchange: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, and MAC: hmac-sha2-512, hmac-sha2-256-96, hmac-sha2-512-96. The new Public Key algorithms are available on the client side only, while the new Key Exchange and MAC algorithms are available on both client and server side (although server side only applies to VLTrader and Harmony). The new Key Exchange algorithms are not available in FIPS mode.

### Enhancements - ebMS

- Added an option to ebXML to modify the format of the Content-Id header.
- Added new ebMS "Allow Incoming Request With Missing Role Element" advanced property, which when enabled allows an incoming request without a role element value to be processed if it otherwise matches a configured ebMS mailbox.

### Enhancements - OFTP

- Added a new OFTP host advanced property "Allow Duplicate SFIDs". Setting this property to True allows files with duplicate SFIDs to be accepted and simply log a message if a duplicate is received.
- Added support for configuring EERP timeouts and resends at the OFTP host level through two new advanced properties: 'Async EERP Timeout (minutes)' and 'Async EERP Resends'. If these values are changed from default, they override the values set in the Local Listener. The REST API has been updated with these new properties and the OFTP property 'outgoing.signEerp' was moved to 'outgoing.receipt.sign'.

### Enhancements - MQ

- Added support for the following MQ SSL cipher specs: ECDHE_RSA_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384.

### Enhancements - SMTP

- Added the ability to configure individual SMTP Proxies to use Start TLS via the property 'Use Start TLS' in the proxy configuration screen. This property defaults to 'True' to match existing functionality.

### Enhancements - S3

- Added support for cross-account access using AWS's AssumeRole feature in the S3 Connector.
- Added new S3 connector property, AccessControlList (ACL), for cross-account use. This new property applies the selected ACL permissions on objects PUT to a bucket.

### Bug Fixes - Framework

- Fixed an issue where cloning a connector host that has a 'System Scheme Name' defined would break directories using the original connector's 'System Scheme Name'.
- Fixed an issue where failed DocumentDB events on disk could be attempted continuously. These events are now moved to a subfolder to allow for investigation and corrective action
- Fixed an issue where api/resourceFolders endpoint would fail after a change was made to a host through the command line. This would impact the WebUI displaying the hosts.
- Upgraded BouncyCastle library to 1.70 and upgraded JCIFS-NG library to 2.17.
- Fixed a bug where placing & or && after LREPLACE or LDELETE commands would cause the action to fail when run through the REST API.
- Fixed an issue where generating a User certificate with a DSA key would fail.
- Fixed an issue, introduced in 5.7.0.0, where importing a User certificate with a DSA key would fail.

- Fixed an issue where connecting to the WebUI through a HTTP/s port with FIPS mode enabled would cause the web browser to report a cipher error and prevent the page from loading.
- Fixed an issue where updating a host's certificate through REST API would set the host to 'Not Ready' when the certificate is a PGP key-generated certificate.

### Bug Fixes - AS2

- Fixed an issue where, if the AS2 Receipt-Delivery-Option header contained a username:password in the URL, it would fail to send the MDN to the trading partner.

### Bug Fixes - FTP

- Fixed a problem where, if the FTP AUTH TLS command (or variant) should throw an exception and command retries are in effect, the command would not be re-invoked.
- Fixed an FTPs Active mode issue introduced in 5.7.0.0 where, when the 'SSL Maximum Protocol Version' was set below the new maximum of 'TLS 1.3', it would fail to find an open data port in the specified range or it would fail in SSL negotiation.

### Bug Fixes - HTTP

- Fixed an issue where SSL connections could fail with a NullPointerException when SSL Debug was enabled.

### Bug Fixes - SSH FTP

- Fixed a potential SFTP server problem where a file stat request would not return a response. This could occur after a file upload, if a file stat request from a client occurred at the same time that the file was deleted or moved by the server.
- Fixed an issue where, if the trading partner's SSH server prematurely closed a client connection during the initial protocol version negotiation, the result could be excessive CPU usage up to the configured connection timeout.
- Cleo Harmony and Cleo VLTrader only: Fixed an issue introduced in 5.6.2.8 where a zero-byte file uploaded through SFTP would not be written to disk.

### Bug Fixes - Portal

- Cleo Harmony and Cleo VLTrader only: Fixed an issue with SAML authentication where IDP-initiated login would sometimes fail when using a Chromium-based browser.
- Cleo Harmony and Cleo VLTrader only: Fixed an issue where a user password change through Cleo Portal could be lost if an admin was updating the user's mailbox at the same time.

### Bug Fixes - File

- Cleo Harmony and Cleo VLTrader only: In the File connector, for Windows, the DIR command no longer shows inaccessible directories.

### Bug Fixes - SMB

- Cleo Harmony and Cleo VLTrader only: Fixed a small memory leak in the SMB connector when sending or receiving an SMB file.
- Cleo Harmony and Cleo VLTrader only: Fixed an issue where the SMB connector would fail when connecting to AS400 IFS SMB shares with the following error: "TreeID is invalid".

- Cleo Harmony and Cleo VLTrader only: Fixed a bug where VersaLex would not start up if FIPS was enabled due to an issue with the SMB connector. Also, fixed an issue with the SMB connector connecting to shares in FIPS mode.

### Bug Fixes - AzureBlob

- Fixed a bug where SFTP transfers would hang if the file was an AzureBlob and the client tried to set the file time.
- Fixed an issue where users would not be able to CD into a subdirectory of an Azure Blob connector when the Azure Blob container was set up as Data Lake Storage.

# Fixed issues in version 5.8.0.1

### Enhancements - Framework

- Added support for getting/setting all applicable connector host advanced properties through the REST API.

### Enhancements - Portal

- Added support for getting/setting all applicable connector host advanced properties through the REST API.

### Bug Fixes - Framework

- Fixed an issue where the WebUI would fail to launch after a Javascript action was run on Windows.
- Fixed an issue where user mailboxes using LDAP connectors were sometimes counting an extra user against the license. This could potentially cause some licensed mailboxes to be automatically disabled.
- Fixed an issue where the DocumentDB would not start correctly if the system did not have access to the internet. Also, fixed an issue where spaces in the directory path for VersaLex on Windows would cause the DocumentDB to not start.
- Fixed a problem when generating an X509 certificate with or from an OpenPGP keyring where the master key expiration was not being set.
- Fixed a problem when re-receiving a transfer that was locally packaged where the content would be locally packaged a second time (i.e. double encrypted).
- Fixed an issue where including non-ASCII characters in the VLTransfers.ResultText database field could cause the value to be too large for the database. All entries are now truncated to the correct length regardless of included chars.

### Bug Fixes - SSH FTP

- Fixed a problem during diffie-hellman-group-exchange-sha256 key exchange where VersaLex was incorrectly ignoring a reply message, causing the next message read to be unexpected and resulting in an InvalidMessageException.

### Bug Fixes - S3

- Fixed an issue that could cause a BadDigest when uploading files from the S3 connector if the incoming buffer is not divisible by 1024 bytes.

### Security - Framework

- Fixed an issue where clients were able to negotiate elliptical curve ciphers outside of the VersaLex Local Listener settings. Also removed deprecated named elliptical curves from the Local Listener according to RFC 8422. Lastly, VersaLex now honors the existing Local Listener advanced property "SSL Ignore Client Cipher Preference Order" for elliptical curve ciphers as well. Note: VLProxy 3.10.0.1 is required if using VLProxy.

# Fixed issues in version 5.8.0.2

### Enhancements - SSH FTP

- Added support for ECDSA and Ed25519 algorithms during SFTP key authentication for both client and server connections. ECDSA and Ed25519 keys can be imported or generated, but note that these can only be used with SFTP. Ed25519 is not supported in FIPS mode. Note: VLProxy 3.10.0.2 is required if using VLProxy.

### Bug Fixes - Framework

- Fixed an issue where 'System Scheme Name' property on a connector host would be cleared when syncing to another node.
- Fixed a problem where ExecuteOn for a specific mailbox was being limited to three concurrent execution threads (e.g. ExecuteOnSuccessfulReceive for a user mailbox).

## Fixed issues in version 5.8.0.3

No updates for Cleo LexiCom in this patch release.

# Fixed issues in version 5.8.0.4

### Enhancements - SSH FTP

- On the SFTP client side, added support for the ssh-ed25519 public key algorithm. This algorithm is not supported in FIPS mode.

# Fixed issues in version 5.8.0.5

### Enhancements - SSH FTP

- On both the SFTP client and server sides, added support for the rsa-sha2-256 and rsa-sha2-512 public key algorithms. Note: VLProxy 3.10.0.3 is required if using VLProxy.

# Fixed issues in version 5.8.0.6

### Bug Fixes - Framework

- Fixed an issue where OpenPGP unpackaging could fail depending on the packaged file size.

### Bug Fixes - SSHFTP

- Fixed a problem where a valid regular expression configured for one of the system level Client SSH FTP Pattern properties could cause no client algorithms to be listed at runtime depending on which algorithms match the regular expression.

# Fixed issues in version 5.8.0.7

### Bug Fixes - Framework

- Fixed an issue where a CA store certificate that was previously browsed and selected for configuration (e.g. OpenPGP encryption/signature verification certificate) was not being properly re-selected for the same configuration when re-browsing.

# Fixed issues in version 5.8.0.8

### Enhancements - Framework

- Removed a warning message that would appear when sending bundled Database Payload and setting the property 'Clear.Set.Properties' in the VLOutgoingProperties table.

## Fixed issues in version 5.8.0.9

No updates for Cleo LexiCom in this patch release.

# Fixed issues in version 5.8.0.10

### Enhancements - RNIF

- Added support for CIDX (Chemical Industry Data eXchange). CIDX can be enabled in an RNIF host by selecting 'RNIF Version' v1.1 and selecting the 'CIDX' checkbox. A new 'Incoming content format', MIME, has been added which will store the incoming MIME data instead of just the service content. A new Advanced property, Save Received Ack As Payload, has also been added. Enabling this property will copy the Received Ack into the Inbox and Receivedbox.

  **Note:** VLProxy 3.10.0.7 is required if using VLProxy.

## Fixed issues in version 5.8.0.11

No updates for Cleo LexiCom in this patch release.

## Fixed issues in version 5.8.0.12

### Bug Fixes - Framework

- Fixed an issue where a certificate could appear to be missing causing exceptions when listing certificate through the REST API.
- When not polling for files, can no longer set a new schedule for an action to run continuously. The schedule recurrence must now be at least 5 seconds.

### Bug Fixes - FTP

- When the Security Mode in an FTPs host is changed to none, the Advanced "Explicit SSL Post Command" property value is now cleared if it is still set to the default of "PBSZ 0;PROT P". Refer to the Explicit SSL Post Command documentation for more information.

# Fixed issues in version 5.8.0.13

### Enhancements - SSH FTP

- Added a new SSH FTP "Large File Transfer" property. It uses a large window size and sends a simple@putty.projects.tartarus.org channel request to the server indicating that the server should also use a large window size, as there will only be one channel open on the connection.

### Bug Fixes - Framework

- Added a warning message to the top of the Certificate Exchange dialog if a scheduled certificate exchange/update is being delayed because the dialog is open.

### Bug Fixes - AzureBlob

- Fixed an issue with the AzureBlob connector where the connector would use the default HTTP/s system forward proxy if a proxy was not configured in the connector itself. This left no way to opt out of using the default proxy. Now the default proxy does not apply to the AzureBlob connector and a proxy must be explicitly configured in the connector.

## Fixed issues in version 5.8.0.14

### Enhancements - Framework

- Upgraded Apache Log4j library to version 2.22.0

### Enhancements - HTTP

- Added the ability to use macros in the source of HTTP and HTTP/s actions.

# Fixed issues in version 5.8.0.15

### Enhancements - Framework

- If there is an error reading an XML config file and it's not a syntax exception, the stack trace of the causing exception is now logged to assist in diagnosis.
- PGP certify, sign, and encrypt key usage flags are now being set (refer to https://www.rfc-editor.org/rfc/rfc4880#section-5.2.3.21). These flags may be required by other software packages when exchanging PGP keys.

### Enhancements - RNIF

- Removed RNIF 1.1 Content-Type header check for "version=1.0" so it is compatible with systems that do not send the version.

### Bug Fixes - Framework

- Modified generated aliases for temporary actions of connectors to use a random string of characters rather than the time in milliseconds to ensure unique aliases are created.
- When running VersaLex commandline, eliminated a "WARN StatusConsoleListener" deprecation warning that would be printed multiple times to the console at the beginning of execution. This warning started appearing with version 5.8.0.14.

# Fixed issues in version 5.8.0.16

### Enhancements - Framework

- Added a REST API endpoint, /api/authentication/refresh, which allows for a new access token to be issued using a refresh token which is provided along with the access token. This enables the WebUI to get a new access token preventing a user from being logged out when the access token expires.

### Bug Fixes - Framework

- Fixed an issue where a certificate signing request (CSR) could not be generated on a user certificate with an ECDSA or ED25519 private key.

# Fixed issues in version 5.8.0.17

### Bug Fixes - Framework

- Fixed a problem where a PKCS#12 certificate/private key using the ECDSA or Ed25519 algorithm could not be imported. Note: Ed25519 is not supported in FIPS mode. Also fixed a problem in FIPS mode where a missing cryptography library was causing all PKCS#12 imports to fail.

# Fixed issues in version 5.8.0.18

### Enhancements - Framework

- Fixed an issue where importing a PKCS#12 file would fail if the certificate was generated with a brainpool elliptic curve.

### Enhancements - SSH FTP

- Added support for hmac-sha2-256-etm@openssh.com and hmac-sha2-512-etm@openssh.com algorithms for both client and server SFTP connections. Note: VLProxy 3.10.0.10 is required if using VLProxy.

# Fixed issues in version 5.8.0.19

### Enhancements - Framework

- Macro replacement is now supported in a wildcarded GET or LCOPY command source. Note that macro replacement is still not supported in a source containing a regular expression.

### Enhancements - RNIF

- Added option 'Add Filename to Attachment Content Type' for RNIF to add the filename of the attachment to the Content-Type MIME header.

### Bug Fixes - Framework

- Fixed an issue where the Certificate Signing Request generated for an ECDSA certificate had an invalid signature.

# Fixed issues in version 5.8.0.20

### Bug Fixes - Framework

- Fixed an issue with the Web UI where users could still schedule actions to run continuously without polling for files.

### Security - Framework

- Fixed a vulnerability which could lead to injection of malicious JavaScript.

## Known issues in version 5.8.0.20

- In Certificate Manager, when exporting a user certificate and private key to a PKCK#12 file, "Enable strong protection" must be selected. Otherwise, the export will fail.

# Fixed issues in version 5.8.0.21

### Security - Framework

- Address additional discovered potential attack vectors of the identified unrestricted file upload and download vulnerability (CVE-2024-50623). After applying the patch, the system logs an error if a file is detected as previously modified (and has been restored). If detected, the error log will also be emailed to the System Administrator. Please ensure to configure a System Administrator email address in system options before applying the patch.

### Enhancements - Framework

- Improved performance when mailboxes are configured using a LDAP connector for authentication.

### Bug Fixes - Framework

- Removed an error message from being logged for stale WebUI sessions. This was introduced in 5.8.0.20.
- Cleo Harmony and Cleo VLTrader only: In the FIPS edition, fixed an issue where configured passwords were considered invalid when not in FIPS mode. This issue was first introduced in 5.8.0.18.
- Fixed an issue where an Authenticator Connector error could result in VLProxy failing to receive user data correctly (which prevents VLProxy from starting correctly) and VersaLex failing to load the host that had the error.
- Cleo Harmony and Cleo VLTrader only: Fixed an issue where triggered actions that are part of a connector host would not show up in the Transfers page in the WebUI.

### Bug Fixes - RNIF

- Fixed an issue in RNIF 1.1 where 'inReponseTo.ActionIdentity.InstanceIdentifier' in the acknowledgement did not match the original Request/Response message.

# Fixed issues in version 5.8.0.22

### Bug Fixes - Framework

- Fixed an issue where users would not be able to log in if an LDAP connector was invalid and used to authenticate users in a Users host.

# Fixed issues in version 5.8.0.23

### Bug Fixes - Framework

- Added extra synchronization when reading and updating the schedule to prevent possible loss of scheduled items.
- Removed the option to disable strong protection when exporting user certificate and private key due to weak protection no longer being supported.

## Fixed issues in version 5.8.0.24

### Security - Framework

- Addresses a critical vulnerability which exploits the ability for unrestricted file upload and download and execute malicious host definitions in the product (CVE pending). After applying the patch, errors are logged for any files found at startup related to this exploit, and those files are removed.

# Fixed issues in version 5.8.0.25

### Bug Fixes - Framework

- Fixed an issue where syncing receipts would fail with a `403 Forbidden` if the receipt storage location was set to an absolute folder path. This was introduced in 5.8.0.24.
- Fixed an issue where a NullPointerException could be thrown if there was an issue listing folders while doing file cleanup at startup. This was introduced in 5.8.0.24.

# Fixed issues in version 5.8.0.26

### Bug Fixes - Framework

- Fixed an issue where a mailbox could be counted twice for licensing resulting in the mailbox being disabled.
- Fixed an issue where licenses for specific protocols would not count User mailbox's correctly causing mailboxes to be disabled.

### Bug Fixes - Portal

- Changed Portal SAML authentication storage to clear when the Portal page is closed.

### Security - Framework

- This update contains other security-related improvements. For customer protection, Cleo does not disclose all security update details. For further information, please contact customer support. For critical security updates or if there is a known exploit, Cleo will publish a security bulletin and notify customers.

# Fixed issues in version 5.8.0.27

### Bug Fixes - HTTP

- Fixed an issue in HTTP/s hosts (e.g. AS2, ebMS, ...) where the `SET ReuseSSLSessionsAcrossActions=False` command was having no effect (i.e. the action's SSL/TLS sessions would still be reused across actions).

### Security - Framework

- This update contains security-related improvements. For customer protection, Cleo does not disclose all security update details. For further information, please contact customer support. For critical security updates or if there is a known exploit, Cleo will publish a security bulletin and notify customers.

## Fixed issues in version 5.8.0.28

### Bug Fixes - ebMS

- Fixed an issue where the ebXML Message Service was only accepting requests that used an "xlink" namespace prefix.