Connect Enterprise UNIX 2.5.0.3iFix7
Cumulative Maintenance
As of 02/05/2015

This maintenance package contains all fixes and enhancements to date for Connect:Enterprise 2.5.0.

Maintenance for Connect:Enterprise UNIX 2.5.0 has been posted on our FixCentral download site. Follow the links in Section 1 to download the packaged maintenance via your browser. Alternatively, follow the instructions in Section 1 to download the maintenance directly to your CEUNIX $CMUHOME directory. Follow the links in Section 2 to read about individual fixes.

NOTE: THIS MAINTENANCE PACKAGE IS A COMPLETE PRODUCT INSTALL.

CONTENTS

Section 1. Downloading the Maintenance

Maintenance for Connect:Enterprise UNIX has been packaged and posted on our Fix Central server. Follow the links to download the packaged maintenance via your browser. README files contain installation instructions.

Download All Available Fixes for CEU 2.5.0 (CEU250 Patch 3 iFix7 BUILD 86) to $CMUHOME

- To pull the CEU250 packaged maintenance to your $CMUHOME directory, follow these instructions:
- Point your browser to
- http://www-933.ibm.com/support/fixcentral/
- Follow the instructions in the README file(s) to get the binaries and install the maintenance.

Back to Contents

Section 2. Fix Index

These fixes are new since GA BUILD 49, posted 3/22/2011. They are all documented further below.

Fixes (BUILD 86 - posted 02/05/2015)

- IT06953 PSIRT 2635 (Upgrade to OpenSSL 0.9.8ze)

Fixes (BUILD 84 - posted 12/19/2014)

- IT06192 Fixing OpenSSL 0.9.8zc on Linux

Fixes (BUILD 83 - posted 11/14/2014)

- PSIRT 2290 POODLE Ability to turn off SSLv3 if -Dtlsonly=true set

Fixes (BUILD 81 - posted 10/30/2014)

- IT05142 - (ADMIN) security findings against Connect:Enterprise

Fixes (BUILD 80 - posted 10/15/2014)

- IT04916 - (AS2) Caught exception reading/parsing the private key for AS2 connection

Fixes (BUILD 79 - posted 09/10/2014)

- IT04315 - (UTIL) Bad protocols showing in CE_STATS_LOG

Fixes (BUILD 78 - posted 08/22/2014)

- IT03813 - (SFTP) Autoconnect fails on files > 64 characters

Fixes (BUILD 77 - posted 08/05/2014)

- IT03577 - (AS2) CE Unix 2.5 AS2 outbound connection issue after connection failed with remote partner due to insufficient space at remote side

Fixes (BUILD 76 - posted 07/16/2014)

- IT03128 - (CORE) Exit daemon terminates; Bad size on SIPS packet

Fixes (BUILD 75 - posted 07/02/2014)

- IT02959 - (FTP/SSH) Remote FTP/SSL PUT failed

Fixes (BUILD 74 - posted 06/16/2014)

- PSIRT 1790 - (CORE) OpenSSL upgrade to 0.9.8za level
- IT00294 - (UTIL) SCC is missing autoconnect failure records

Fixes (BUILD 73 - posted 03/18/2014)

- IT00271 - (UTILS) error during ceukey -r execution - bus error (coredump)

Fixes (BUILD 72 - posted 02/11/2014)

- IC99126 - (FTP/SSH) Connect:Enterprise protocol daemons just drop off
- IC99070 – (AS2) err: could not determine url for outbound request

Fixes (BUILD 71 - posted 01/31/2014)

- IC99071 – (FTP/SSH) allowing remote rename regardless of a flag
- IC98383 - (SVID) problem with autoconnects - missing or duplicated records in the acd cmureport pull

Fixes (BUILD 70 - posted 01/13/2014)

- IC98645 - (FTP) Autoconnect sends PROT P/PBSZ commands to a server before security exchange
- IC98647 – (FTP) Autoconnect fails if port 21 is /etc/services is commented out
- IC98646 - (CORE) During periods of high system activity, the log daemon may time out waiting on a log message from a sender for 2 minutes. If the log daemon is allowed to wait that long before timing out, it can cause problems for other log messages waiting to be received.

Fixes (BUILD 69 - posted 09/30/2013)

- IC92328 - (FTP) Autoconnect fails on SSL handshake with trace level set to 9
- IC91551 - (UTIL) CEU Administration Tool Autocomplete HTML Attribute Not Disabled
- IC92297 - (UTIL) Using Site Administration Tool will truncate "mailbox_list" in RSD update
- IC93310 - (UTIL) cmusslverify sort order problem using OpenSSL toolkit
- IC94933 - (UTIL) Upgrade Failure - Encryption Keys Problem - ceukey -R Error=16!
- IC95994 - (UTIL) cmusslverify: error -1: parsing certificates on Solaris
- RT364285- (CORE) cmuconnect -v fails: Already at MAX of 32
- IC91387 - (CORE) Port scanning causing premature daemon termination
- IC94395 - (CORE) CEU limits the cmureport records returned to SCC to 5000
- RT366869 - (CORE) Upgrade OpenSSL-0.9.8y
- (CORE) Upgrade to JRE 1.6 SR14 level

Fixes (BUILD 68) - posted 02/22/2013)

- IC91419 - (UTIL) cmusslgencsr generated private key in RSA format that Certicom toolkit could not handle

Fixes (BUILD 67 - posted 01/02/2013)

- QC17829 - (CORE) Memory leak in SIPS Encryption after CEU2500
- QC17845 - (UTIL) ceupassencrypt utility fails when rsd path is long
- QC19069 - (MBOX) Speed up queries for transmittable batches
- QC19140 - (MBOX) Mailbox child processes hanging after DMZ protocol processes gone
- QC19383 - (UTIL) cmustatus failure turning on T and D flags when one flag already on.
- QC19681 - (CORE_UTILS) proper handling of global key
- QC19841 - (SSH) Flood of log events
- QC19747 - (ASYNC) CEU creating corrupt trace filenames when Async modem fails
- QC20139 - (FTP) Change default behavior on close_notify
- QC20140 - (CORE) cmuconnect command failed with resource not found - Problem with PollDaemon value not being honored correctly

Fixes (BUILD 65 - posted 10/19/2012)

- QC20196 - (UTIL) Fileagent stops caching files until previous cache files are completed.
- QC20019 - (UTIL) ceupassencrypt migration handling of global keys
- QC20417 - (UTIL) cmulist command fail after upgrade - A0x0001 - C0x0204: Session not open - connect() system call failed
- QC20483 - (FTP) subcommand 'user' did not work
- QC20851 - (FTP) FTP_PUT_OPTIONS ID value is not honored during upload
- RTC313659 - (SSH) Autoconnect not retrieving remote file with apostrophe (single quote) in filename

- RTC320247 - (FTP) PASV command with incorrect arguments entered via quote was not parsed correctly
- RTC322258 - (UTIL) ceupassencrypt does not process comments properly
- RTC345786 - (CORE) jetty upgrade to 6.1.26
- IC85609 - (FTP) FTP child process spawn into a loop awaiting at least 4 bytes on the cntrl channel
- IC86162 - (SSH) Batches with flag "D" are renamed during remote connect
- IC86578 - (SSH) Autoconnect session does not timeout when waiting password reply from server
- IC86497 - (SSH) RMT_INFO ADD record to not written to report when client attempt to use fsetstat
- IC86885 - (SSH) File (known_hosts) is created with the wrong permissions when traces are running
- CVE-2012-2333 - Upgrade to OpenSSL 0.9.8.x

Back to Contents

List of fixes by category

FTP related fixes

- QC20139 - (FTP) Change default behavior on close_notify
- QC20483 - (FTP) subcommand 'user' did not work
- QC20851 - (FTP) FTP_PUT_OPTIONS ID value is not honored during upload
- RTC320247 - (FTP) PASV command with incorrect arguments entered via quote
- was not parsed correctly
- IC85609 | (FTP) FTP child process spawn into a loop awaiting at least 4 bytes on the control channel
- RT366869 - (CORE) Upgrade OpenSSL-0.9.8y
- IC98645 - (FTP) Autoconnect sends PROT P/PBSZ commands to a server before security exchange
- IC98647 – (FTP) Autoconnect fails if port 21 is /etc/services is commented out

Back to Contents

SSH related fixes

- QC19841 - (SSH) Flood of log events
- RTC313659 - (SSH) Autoconnect not retrieving remote file with apostrophe (single quote) in filename
- IC86162 - (SSH) Batches with flag "D" are renamed during remote connect
- IC86578 - (SSH) Autoconnect session does not timeout when waiting password reply from server

- IC86497 - (SSH) RMT_INFO ADD record to not writhen to report when client attempt to use fsetstat
- IC86885 - (SSH) File (known_hosts) is created with the wrong permissions when traces are running
- IC99126 - (FTP/SSH) Connect:Enterprise protocol daemons just drop off
- IC99071 – (FTP/SSH) allowing remote rename regardless of a flag
- IT03813 - (SFTP) Autoconnect fails on files > 64 characters

Back to Contents

AS2 Related fixes

- IC99070 – (AS2) err: could not determine url for outbound request
- IT04916 - (AS2) Caught exception reading/parsing the private key for AS2 connection
- IT03577 - (AS2) CE Unix 2.5 AS2 outbound connection issue after connection failed with remote partner due to insufficient space at remote side

Back to Contents

Core Daemon, General fixes

- QC17829 - (CORE) Memory leak in SIPS Encryption
- QC19069 - (CORE) Updated Mailbox ACL code to recognize new search operation
- QC19140 - (MBOX) Mailbox child processes hanging after DMZ protocol processes gone
- QC19383 - (UTIL) cmustatus failure turning on T and D flags when one flag already on.
- QC20140 - (CORE) cmuconnect command failed with resource not found - Problem with PollDaemon value not being honored correctly
- RTC345786 - (CORE) jetty upgrade to 6.1.26
- IC98646 - (CORE) During periods of high system activity, the log daemon may time out waiting on a log message from a sender for 2 minutes. If the log daemon is allowed to wait that long before timing out, it can cause problems for other log messages waiting to be received.
- IC98383 - (SVID) problem with autoconnects - missing or duplicated records in the acd cmureport pull
- PSIRT 1790 - (CORE) Security advisory. Man-in-the-middle vulnerability fix
- IT03128 - (CORE) Exit daemon terminates; Bad size on SIPS packet
- PSIRT 2290 POODLE Ability to turn off SSLv3 if -Dtlsonly=true set
- IT06192 Fixing OpenSSL 0.9.8zc on Linux
- IT06953 PSIRT 2635 (Upgrade to OpenSSL 0.9.8ze)

Back to Contents

Offline Utility, File Agent, API fixes

- QC17845 - (UTIL) ceupassencrypt utility fails when rsd path is long
- QC19681 - (UTIL) proper handling of global key

- QC20196 - (UTIL) Fileagent stops caching files until previous cache files are completed.
- QC20019 - (UTIL) ceupassencrypt migration handling of global keys
- QC20417 - (UTIL) cmulist command fail after upgrade - A0x0001 - C0x0204: Session not open - connect() system call failed
- RT279571- (UTIL) ceupassencrypt does not process comments properly
- IT00294 - (UTIL) SCC is missing autoconnect failure records
- IT00271 - (UTILS) error during ceukey -r execution - bus error (coredump)
- IT04315 - (UTIL) Bad protocols showing in CE_STATS_LOG

Back to Contents

Web Admin Tool / Reporting fixes

- IT05142 – (CEUADMIN) security findings against Connect:Enterprise

Back to Contents

Async Daemon fixes

- QC 19747 (ASYNC) CEU creating corrupt trace filenames when Async modem fails

Back to Contents

Bisync Daemon fixes

None

Back to Contents

Section 3. Detailed Fix Descriptions (by Fix Number)

Section 3 lists detailed information about each fix listed in Section 2. Fixes are in numerical order by fix number.

Back to Contents

QC17829 - (CORE) Memory leak in SIPS Encryption after CEU2500

Customer upgraded to CEU2500 running with SIPS encryption. When pulling a large file (>250MB), the mailbox child process failed with an out of memory condition. There was a memory leak in the SIPS encryption code causing large files to use up all existing memory and fail.

Resolution: Updated the SIPS encryption code to free the encryption buffers that it obtains for every packet.

QC17845 - (UTIL) ceupassencrypt utility fails when rsd path is long

Customer attempting to run ceupassencrypt against rsd filename that is over 80 characters including the path. The filename gets truncated at 80 bytes and the ceupassencrypt command fails.

Resolution: Updated the ceupassencrypt code to use a 512 byte buffer for the rsd file pathname instead of an 80 byte buffer.

QC19069 - (MBOX) Speed up queries for transmittable batches

Customer is doing queries against very large mailboxes (>50k batches in each mailbox id). The queries specify the flags -FR!D!T!I!P!V which limits the query to transmittable batches, but the query operations take 15-20 seconds or more to complete.

Resolution: Created a new query operation which gets used when the caller specifies -FR!D!T!I!P status flag filters. The new operation only reads the transmittable batches using the TRID or TRIDBID indexes, which keep the transmittable batches sorted at the front. In most cases, the query now executes in a few milliseconds.

QC19140 - (MBOX) Mailbox child processes hanging after DMZ protocol processes gone

Customer found that some mailbox processes (cmumboxd) were showing up in the system process displays long after the associated DMZ protocol sessions were gone. Traces showed that the original request had been processed and the mailbox was waiting for another. It is possible that the DMZ firewall was silently cutting the socket after 5 minutes such that the mailbox daemon was not notified of the disconnect.

Resolution: Set a timeout in the mailbox daemon while waiting for the next operation. If the caller does not request a new operation within 30 minutes, the mailbox child process ends.

QC19383 - (UTIL) cmustatus failure A0x0305 – C0x0305

Behavior change cause by QC19000. After applying the fix for defect QC19000, the Customer found that when they did a cmustatus command to turn on the D and T flags, the utility ignored batches that already had one or the other flag already on.

Resolution: Implemented a list to keep track of records that server returns and each new record is being checked against the list to prevent duplication

QC19681 - (CORE_UTIL) after upgrade from 2.4.03 to 2.5.0 customer was unable to upload batch using 3DES batch encryption

Resolution: fixed handling of global keys, allowing now them to have '\0' characters inside and fixed case when at migration from 2.4.03 to 2.5.0 when there was no deskey in 2.4.03, the deskey in 2.5.0 was created incorrectly

QC19747 (ASYNC) When an ASYNC modem fails to connect, CEU creates corrupted trace filenames

Resolution: Trace files names are created only after session is established and has a meaningful name

QC19841 - (SSH) Flood of log events

If the client keeps sending invalid request, CEU is designed to log it, and if the authenticated client is looping, it makes it effectively a DoS attack and the amount of log records could bring the system down.

Resolution: A new environmental variable SSH_CONSECUTIVE_FAILURES_LIMIT has been added for CEU administrator to set the number of consecutive failed attempts after which CEU will close the session and log the client off.

In this case a new error log record will be logged: RC_TOO_MANY_FAILURES (0x005C). If the environmental variable SSH_CONSECUTIVE_FAILURES_LIMIT is omitted, default value is set to 1024.

QC 20019 (UTIL) ceupassencrypt migration handling of global keys

When passwords were encrypted other than RC4, ceupassencrypt migration tool could not handle retrieving of global keys.

Resolution: global key uses only RC4 encryption regardless of password encryption

QC 20139 (FTP) Change default behavior on close_notify

After upgrade to CEU2500, SSL sessions with some third party client and server software hang during close_notify at the end of a data operation.

Prior versions of CEU work. Each data socket is secured with SSL/TLS, and at the end of the transfer, CEU begins closing the SSL data socket and sends a close_notify to the other side. We expect to receive one back, but do not get one until a 5-minute timeout has expired.

Resolution: The problem is actually a bug on the remote client or server software. It should respond correctly to our close_notify at the end of the data operation. However, we made 2 updates:

1) Updated ssl_close logic to properly send and check for close_notify from peer. Included debug messages at level 10 to determine if the remote is playing by the rules.

2) If "export NO_WAIT_FOR_PEER_SSL_SHUTDOWN=1" is included in ceustartup prior to the cmuftpd daemon startup, CEU will skip waiting for the remote to send the close_notify and get around the hang condition. This is considered a workaround until the remote software can be fixed to properly respond to the close_notify.

To make life easy for user, it is better to close sockets by default and not to wait for close_notify. In case somebody likes old way there will be env variable WAIT_FOR_PEER_SSL_SHUTDOWN

QC20140 (Core) cmuconnect command failed with resource not found

Problem with PollDaemon value not being honored correctly

Resolution: Instead of hardcoded value of 60 sec, now Control daemon sends ping at polling interval from control.mcd

QC20196 (UTIL) Fileagent stops caching files until previously caches files are completed

Fileagent had to finish all cached tasks, before checking staging directory for new tasks, which leads to a situation, when one long process held the processing when there were free slots to start new tasks, but files in stage directory were not cached

Resolution: The logic of fileagent has been changed. Now, instead of sleeping until all processes end, it wakes up and if the interval allows, it checks stage directory for new arrivals

QC20417 (UTIL) cmulist command fail after upgrade – A0x0001 – C0x0204: Session not open – connect() system call failed

Resolution: Fixed garbled lines when ceupassencrypt used to convert the whole directory with –r* parameter

QC20483 (FTP) FTP command (user) fails logon after first successful logon when using the same session - Error lostconn

When a user logs into FTP and then attempts to login as a different user, they get "Error lostconn" and the session is lost. An earlier fix to use the same mailbox socket for all operations was erroneously closing socket 0 when the USER command was issued.

Resolution: Updated the mailbox close logic to bypass the socket close when the socket number is zero, since that is always STDIN on the FTP command channel.

QC20851 (FTP) FTP_PUT_OPTIONS ID value is not honored during upload

FTP_PUT_OPTIONS option is RSD file is supposed to redirect the upload file into mailbox, specified by ID keyword of FTP_PUT_OPTIONS. But the parser of the FTP_PUT_OPTIONS line processed the line with 2 id words: from FTP_PUT_OPTIONS and main mailbox id. And the last id in the line was used as mailbox ID.

Resolution: The parsing order of an original ID and redirected ID was reversed and now if the redirected ID is specified, the upload is directed into this mailbox ID

RTC322258 (UTIL) ceupassencrypt does not process comments properly

Resolution: ceupassencrypt now processes comments properly

RTC320247 (FTP) PASV command with an argument caused FTP replies to get out of sync

A Customer made network changes and began to have FTP session failures. One of the new appliances on the network was translating a "EPSV ALL" (extended passive mode) command to "PASV ALL". The CEU FTP server did not expect arguments with the PASV command, but instead of sending one 500 error reply, it sent two, causing all subsequent replies to be out of sync on the client. Several other commands, which do not allow arguments, also cause the duplicate error replies: ABOR, NOOP, PWD, QUIT, REST, SYST, XPWD.

Resolution: Updated the command parser to ignore any arguments that are included on the PASV command and process the command as if it had no arguments. Made the same change to the parser for the other commands above.

RTC313659(SSH) Autoconnect not retrieving remote file with apostrophe (single quote in filename

CEUnix does not provide logic to deal with files with apostrophe inside. If apostrophe (single quote) happens to be in a file name (which is legitimate), autoconnect fails to deal with such file.

Resolution: Logic of apostrophe processing was added to autoconnect component.

RTC345786 – (CORE) jetty upgrade to 6.1.26

Security advisory. Due to security exposure in jetty 6.1.23, jetty was upgraded to 6.1.26

IC85609 (FTP) FTP child process spawn into a loop awaiting at least 4 bytes on the control channel

When an ftp client sends wrong request (3 letters of action code instead of 4), CEUnix rejects it, but did not disconnects. If the client keeps sending invalid requests, it causes a loop, imitating denial of service attack.

Resolution: After 100 invalid requests, the session gets disconnected, the reason is logged, and trace shows the reason of disconnect.

IC86162 (SSH) Batches with flag "D" are renamed during remote connect

If there were several batches with the same name and some of them marked with D flag (that is marked for deletion) and remote client tried to rename visible batch, all batches with the this name were renamed, including those invisible ones, like marked with D flag.

Resolution: renaming batch now is down with a filter "R!D!T!I!P" to prevent renaming batches that are invisible to a remote client.

IC86578 (SSH) Autoconnect session does not timeout when waiting password reply from server

Autoconnect session is set to wait forever for server password verification and if server does not answer, the session hangs indefinitely.

Resolution: The timeout value that user enters for SSH daemon is used to timeout the wait for server reply

IC86497 (SSH) RMT_INFO ADD record to not written to report when client attempt to use fsetstat

Bitvise SSH client after successful upload issues fsetstat command, which is not supported by CEUnix and this prevents CEUnix to log the record about successful transaction.

Resolution: With any FTP client that uses fsetstat, CEUnix now logs the record about transaction.

IC86885 (SSH) File (known_hosts) is created with the wrong permissions when traces are running

When user starts tracing and there is known_hosts files in ssh directory, autoconnect creates this file with wrong permission (666), because tracing resets permission and never reverts it back

Resolution: known_hosts file should be always created with 644 permission and then resets the mask back to what it was before

CVE-2012-2333 – Invalid TLS/DTLS record attack

Security advisory.

Resolution - Upgrade to OpenSSL 0.9.8.x

RTC364285 - (CORE) cmuconnect -v fails: Already at MAX of 32

When cmuconnect is used in verbose mode, max number of connection was set to 32

Resolution: Max number of connections was increased to 256

IC91387 - (CORE) Port scanning causing premature daemon termination

CEU daemons communicate between themselves via sockets and if there is port scanning happens on the system, daemon got ECONNABORTED error and disconnected.

Resolution: Daemons now keep waiting to accept socket even if there is port scanning going

IC91419 - cmusslgencsr generated private key in RSA format that Certicom toolkit could not handle

cmusslgenscsr utility was generating private key not in PKCS8 format and therefore java Certicom toolkit (that supports AS2 protocol) cannot handle private keys generated by cmusslgencsr

Resolution: cmusslgencsr utility was changed to generate private keys in PKCS8 format

IC91551 - (UTIL) CEU Administration Tool Autocomplete HTML Attribute Not Disabled

CEU Administration Tool Autocomplete HTML Attribute Not Disabled

Resolution: added a function to prevent autocomplete of a password field

IC92297 - (UTIL) Using Site Administration Tool will truncate "mailbox_list" in RSD update

If user changed manually edited rsd file and specified more than 32 mailboxes there and then used ceuadmin GUI - the saved rsd file contains only 32 mailboxes and the rest were chopped without a warning

Resolution: A warning now is issued when the user attempts to save more than 32 mailboxes

IC92328 - (FTP) Autoconnect fails on SSL handshake with trace level set to 9

Upgrading to OpenSSL 0.9.8y caused SSL handshake to fail, because of a bug in OpenSSL certificate printing

Resolution: The code was changed to circumvent OpenSSL bug

IC93310 - (UTIL) cmusslverify sort order problem using OpenSSL toolkit

cmusslverify utility was using OpenSSL for printing chain of trusted certificates and OpenSSL sorts certificates in order of hashed CN field, which is effectively random order and it was not convenient to maintain trusted certificate file.

Resolution: cmusslverify now prints certificates in order they are maintained in a trusted file. Also, a new parameter (-e=xxx) was added to check expiration dates of certificates for xxx days ahead.

IC94395 - CEU limits the cmureport records returned to SCC to 5000

Resolution: The limit was increased to 25000

IC94933 - (UTIL) Upgrade Failure - Encryption Keys Problem - ceukey -R Error=16!

Conversion of 2.4.02 keys failed at upgrade to 2.5

Resolution: Improved diagnostic of a ceukey utility. Now if the decryption of a global key is successful, ceukey prints a message: "The current passphrase has been successfully validated"

IC95994 - (UTIL) cmusslverify: error -1: parsing certificates on Solaris

After successfully listing trusted certificates, the Sun version of cmusslverify prints the erroneous error message

Resolution: Corrected the return status so that the erroneous error message would not be printed

RT366869 - (CORE) Upgrade OpenSSL-0.9.8y

Security advisory.

Resolution - Upgrade to OpenSSL 0.9.8y

(CORE) Upgrade JRE package to 1.6 SR14 level

Resolution – Upgrade JRE to 1.6 SR14 level

IC98645 - (FTP) Autoconnect sends PROT P/PBSZ commands to a server before security exchange

Autoconnect sends PROT P/ PBSZ commands to a server before security exchange to accommodate Filezilla servers, but it it breaks other server

Resolution: Environmental variable FTP_PBSZ_BEFORE_SECURITY_XCHANGE has been implemented. If it is set - ftp sends PROT B/PBSZ before security exchange, if not - then they are sent after security has been established

IC98647 - (FTP) Autoconnect fails if port 21 in /etc/services is commented out

Resolution: Bypass checking whether ftp service is running, because it is redundant

IC98647 - (CORE) During periods of high system activity, the log daemon may time out waiting on a log message from a sender for 2 minutes. If the log daemon is allowed to wait that long before timing out, it can cause problems for other log messages waiting to be received.

Resolution: Changed the timeout value for receiving the log message on a socket from 120 seconds to 5 seconds.

IC98383 - (SVID) problem with autoconnects - missing or duplicated records in the acd cmureport pull. When Sterling Control Center monitors a Connect:Enterprise UNIX instance, it invokes the cmureport command to gather much of its activity data. It depends on the records being returned in ascending time order, so that it can know which data has already been requested. Because of the way the CEU autoconnect detail report information is gathered, the ACDetail report can return records out of order. This can lead to duplicate and missing records in the Control Center database.

Resolution: In the cmusvwd session generated by SCC or the Admin GUI, sort the output of any cmureport acdetail command prior to generating the XML response. Sort on the ending time of the detail records.

IC99071 – (FTP/SSH) allowing remote rename regardless of a flag. During a remote connect, the user attempts to rename a file that was uploaded to the repository. The rename fails because it was unable to locate the batch.

Resolution: Now allow batches to be renamed by SSHFTP even if they don't have the R flag set

IC99070 – (AS2) err: could not determine url for outbound request . AS2 could not determine URL for outbound request. When an outbound AS2 contract configured for secure connection specifies a custom cipher instead of a cipher strength (All or Strong), C:E gets a Java NullPointerException while setting up for the connection. The code that parses the AS2 configuration file was erroneously handling custom cipher selections received.

Resolution: Now correctly handle custom cipher suites for AS2 outbound connections so that contracts can use specific ciphers

IC99126 - (FTP/SSH) Connect:Enterprise protocol daemons just drop off, and no errors or commands listed. Customer getting core dumps in FTP and SSHFTP child processes when running traces and there are problems at the end of session. Various debug messages were not coded correctly, causing the segmentation faults. Also, during reconnect processing with master daemon, the ACD slave socket was not closed completely, and caused the next remote connect session to fail.

Resolution: Corrected debug statements to include all required parms to avoid core dumps
Cleaned up lostpeer processing in the FTP and SSHFTP child processes when connections drop
Ensure ACD slave socket is closed completely during reconnect processing..

IT00271 - (UTILS) error during ceukey -r execution - bus error (coredump). Memory misalignment on HPUX systems happened with OpenSSL 0.9.8y and CEUnix that caused coredump when freeing memory used in OpenSSL APIs.)

Resolution: OpenSSL package was recompiled on HPUX and CEUnix was rebuilt with OpenSSL libraries.

IT00294 - (UTIL) SCC is missing autoconnect failure records. The records seem to be out of order in the logacct.dat file so SCC doesn't see them. cmureport utility does not print the autoconnect record if the session ended before the end of interval, but started before start of interval

Resolution: The code was added to handle the case when the autoconnect session started before the beginning of specified interval (option -B) and ended before the end of specified interval (option -T).

PSIRT 1790 - (CORE) Security advisory. Man-in-the-middle vulnerability fix

Resolution: Upgrade OpenSSL to 0.9.8za level.

IT02959 - (FTP/SSH) Remote FTP/SSL on Linux was failing to execute PUT command.

Resolution: Remote FTP/SSL on Linux was fixed

IT02959 - Remote FTP/SSL PUT fails on Linux (SSL/TLS error)

Resolution: Remote FTP/SSL on Linux was fixed

IT03128 - (Core) Exit daemon terminates; Bad size on SIPS packet. Exit daemon terminated when accept() returned any error, but it does not have to if the error is ECONNABORTED

Resolution: errno ECONNABORTED now does not cause exit daemon to terminate prematurely

IT03577 - (AS2) CE Unix 2.5 AS2 outbound connection issue after connection failed with remote partner due to insufficient space at remote side. AS2 protocol was using requeue parameter erroneously

Resolution: requeue parameter for HTTP and EDIINT protocol has been forced to 0

IT03813 - (SFTP) Autoconnect fails on files > 64 characters. SFTP does not process filenames longer than 64 characters. While 64 is a limit for batch name size, sftp should work like ftp, that is cut batch name to 64, but process the file.

Resolution: restrictions for processing filenames longer than 64 for sftp daemon were removed.

IT04315 - (UTIL) Bad protocols showing in CE_STATS_LOG if the batchid field (e.g. filename) happened to contain a comma, then the comma-delimited report could be misinterpreted by the Admin GUI Sterling Control Center.

Resolution: if the report is comma-delimited, then all commas in the detailed report are replaced with underscore character

IT04916 - (AS2) Caught exception reading/parsing the private key for AS2 connection. AS2 component did not support PBES2 features of private keys

Resolution: Added logic logic to process PBES2 features of private keys

IT05142 - security findings against CEUnix. CEUADMIN code did not invalidate previous sessions

Resolution: CEUADMIN code was fixed adding logic to invalidate previous session at any logon

PSIRT 2290 POODLE Ability to turn off SSLv3 if -Dtlsonly=true set

The CEU ADMIN and HTTP daemons allow SSLv3 sessions by default, while SSLv3 has been shown to have vulnerabilities

Resolution: Add the Java property -Dtlsonly=true to the Java command line in the $CMUHOME/javalib/ceuadmind and cmuhttpd startup scripts to disable the SSLv3 protocol in those daemons.

IT06192 Fixing OpenSSL 0.9.8zc on Linux.

CEU OpenSSL 0.9.8zc was misconfigured on Linux platform

Resolution: OpenSSL libraries on Linux were fixed.

PSIRT 2635 (Upgrade to OpenSSL 0.9.8ze)

Resolution: OpenSSL libraries were upgraded to latest level 0.9.8ze.