



*Full credit is given to the above companies including the OS that this PDF file was generated!*

## **Red Hat Enterprise Linux Release 9.2 Manual Pages on 'OPENSSL\_cleanse.3oss!' command**

**\$ man OPENSSL\_cleanse.3oss!**

OPENSSL\_MALLOC(3oss!)      OpenSSL      OPENSSL\_MALLOC(3oss!)

### NAME

OPENSSL\_malloc\_init, OPENSSL\_malloc, OPENSSL\_zalloc, OPENSSL\_realloc,  
OPENSSL\_free, OPENSSL\_clear\_realloc, OPENSSL\_clear\_free,  
OPENSSL\_cleanse, CRYPTO\_malloc, CRYPTO\_zalloc, CRYPTO\_realloc,  
CRYPTO\_free, OPENSSL\_strdup, OPENSSL\_strndup, OPENSSL\_memdup,  
OPENSSL\_strlcpy, OPENSSL\_strlcat, CRYPTO\_strdup, CRYPTO\_strndup,  
OPENSSL\_mem\_debug\_push, OPENSSL\_mem\_debug\_pop, CRYPTO\_mem\_debug\_push,  
CRYPTO\_mem\_debug\_pop, CRYPTO\_clear\_realloc, CRYPTO\_clear\_free,  
CRYPTO\_malloc\_fn, CRYPTO\_realloc\_fn, CRYPTO\_free\_fn,  
CRYPTO\_get\_mem\_functions, CRYPTO\_set\_mem\_functions,  
CRYPTO\_get\_alloc\_counts, CRYPTO\_set\_mem\_debug, CRYPTO\_mem\_ctrl,  
CRYPTO\_mem\_leaks, CRYPTO\_mem\_leaks\_fp, CRYPTO\_mem\_leaks\_cb,  
OPENSSL\_MALLOC\_FAILURES, OPENSSL\_MALLOC\_FD - Memory allocation  
functions

### SYNOPSIS

```
#include <openssl/crypto.h>

int OPENSSL_malloc_init(void);

void *OPENSSL_malloc(size_t num);

void *OPENSSL_zalloc(size_t num);

void *OPENSSL_realloc(void *addr, size_t num);

void OPENSSL_free(void *addr);

char *OPENSSL_strdup(const char *str);
```

```

char *OPENSSL_strdup(const char *str, size_t s);
size_t OPENSSL_strlcat(char *dst, const char *src, size_t size);
size_t OPENSSL_strlcpy(char *dst, const char *src, size_t size);
void *OPENSSL_memdup(void *data, size_t s);
void *OPENSSL_clear_realloc(void *p, size_t old_len, size_t num);
void OPENSSL_clear_free(void *str, size_t num);
void OPENSSL_cleane(void *ptr, size_t len);
void *CRYPTO_malloc(size_t num, const char *file, int line);
void *CRYPTO_zalloc(size_t num, const char *file, int line);
void *CRYPTO_realloc(void *p, size_t num, const char *file, int line);
void CRYPTO_free(void *str, const char *, int);
char *CRYPTO_strdup(const char *p, const char *file, int line);
char *CRYPTO_strdup(const char *p, size_t num, const char *file, int line);
void *CRYPTO_clear_realloc(void *p, size_t old_len, size_t num,
                           const char *file, int line);
void CRYPTO_clear_free(void *str, size_t num, const char *, int);
typedef void (*CRYPTO_malloc_fn)(size_t num, const char *file, int line);
typedef void (*CRYPTO_realloc_fn)(void *addr, size_t num, const char *file,
                                  int line);
typedef void (*CRYPTO_free_fn)(void *addr, const char *file, int line);
void CRYPTO_get_mem_functions(CRYPTO_malloc_fn *malloc_fn,
                              CRYPTO_realloc_fn *realloc_fn,
                              CRYPTO_free_fn *free_fn);
int CRYPTO_set_mem_functions(CRYPTO_malloc_fn malloc_fn,
                             CRYPTO_realloc_fn realloc_fn,
                             CRYPTO_free_fn free_fn);
void CRYPTO_get_alloc_counts(int *mcount, int *rcount, int *fcoun);
env OPENSSL_MALLOC_FAILURES=... <application>
env OPENSSL_MALLOC_FD=... <application>

```

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining `OPENSSL_API_COMPAT` with a suitable version value, see `openssl_user_macros(7)`:

```
int CRYPTO_mem_leaks(BIO *b);
```

```

int CRYPTO_mem_leaks_fp(FILE *fp);
int CRYPTO_mem_leaks_cb(int (*cb)(const char *str, size_t len, void *u),
                        void *u);
int CRYPTO_set_mem_debug(int onoff);
int CRYPTO_mem_ctrl(int mode);
int OPENSSL_mem_debug_push(const char *info);
int OPENSSL_mem_debug_pop(void);
int CRYPTO_mem_debug_push(const char *info, const char *file, int line);
int CRYPTO_mem_debug_pop(void);

```

## DESCRIPTION

OpenSSL memory allocation is handled by the OPENSSL\_xxx API. These are generally macro's that add the standard C `__FILE__` and `__LINE__` parameters and call a lower-level CRYPTO\_xxx API. Some functions do not add those parameters, but exist for consistency.

OPENSSL\_malloc\_init() does nothing and does not need to be called. It is included for compatibility with older versions of OpenSSL.

OPENSSL\_malloc(), OPENSSL\_realloc(), and OPENSSL\_free() are like the C malloc(), realloc(), and free() functions. OPENSSL\_zalloc() calls memset() to zero the memory before returning.

OPENSSL\_clear\_realloc() and OPENSSL\_clear\_free() should be used when the buffer at addr holds sensitive information. The old buffer is filled with zero's by calling OPENSSL\_cleanse() before ultimately calling OPENSSL\_free().

OPENSSL\_cleanse() fills ptr of size len with a string of 0's. Use OPENSSL\_cleanse() with care if the memory is a mapping of a file. If the storage controller uses write compression, then it's possible that sensitive tail bytes will survive zeroization because the block of zeros will be compressed. If the storage controller uses wear leveling, then the old sensitive data will not be overwritten; rather, a block of 0's will be written at a new physical location.

OPENSSL\_strdup(), OPENSSL\_strndup() and OPENSSL\_memdup() are like the equivalent C functions, except that memory is allocated by calling the OPENSSL\_malloc() and should be released by calling OPENSSL\_free().

OPENSSL\_strncpy(), OPENSSL\_strcat() and OPENSSL\_strlen() are equivalents of the common C library functions and are provided for portability.

If no allocations have been done, it is possible to "swap out" the default implementations for OPENSSL\_malloc(), OPENSSL\_realloc() and OPENSSL\_free() and replace them with alternate versions.

CRYPTO\_get\_mem\_functions() function fills in the given arguments with the function pointers for the current implementations. With

CRYPTO\_set\_mem\_functions(), you can specify a different set of functions. If any of malloc\_fn, realloc\_fn, or free\_fn are NULL, then the function is not changed. While it's permitted to swap out only a few and not all the functions with CRYPTO\_set\_mem\_functions(), it's recommended to swap them all out at once.

If the library is built with the "crypto-mdebug" option, then one function, CRYPTO\_get\_alloc\_counts(), and two additional environment variables, OPENSSL\_MALLOC\_FAILURES and OPENSSL\_MALLOC\_FD, are available.

The function CRYPTO\_get\_alloc\_counts() fills in the number of times each of CRYPTO\_malloc(), CRYPTO\_realloc(), and CRYPTO\_free() have been called, into the values pointed to by mcount, rcount, and fcount, respectively. If a pointer is NULL, then the corresponding count is not stored.

The variable OPENSSL\_MALLOC\_FAILURES controls how often allocations should fail. It is a set of fields separated by semicolons, which each field is a count (defaulting to zero) and an optional atsign and percentage (defaulting to 100). If the count is zero, then it lasts forever. For example, "100;@25" or "100@0;0@25" means the first 100 allocations pass, then all other allocations (until the program exits or crashes) have a 25% chance of failing.

If the variable OPENSSL\_MALLOC\_FD is parsed as a positive integer, then it is taken as an open file descriptor. This is used in conjunction with OPENSSL\_MALLOC\_FAILURES described above. For every allocation it will log details about how many allocations there have been so far,

what percentage chance there is for this allocation failing, and whether it has actually failed. The following example in classic shell syntax shows how to use this (will not work on all platforms):

```
OPENSSL_MALLOC_FAILURES='200;@10'  
export OPENSSL_MALLOC_FAILURES  
OPENSSL_MALLOC_FD=3  
export OPENSSL_MALLOC_FD  
...app invocation... 3>/tmp/log$$
```

## RETURN VALUES

OPENSSL\_malloc\_init(), OPENSSL\_free(), OPENSSL\_clear\_free()  
CRYPTO\_free(), CRYPTO\_clear\_free() and CRYPTO\_get\_mem\_functions()

return no value.

OPENSSL\_malloc(), OPENSSL\_zalloc(), OPENSSL\_realloc(),  
OPENSSL\_clear\_realloc(), CRYPTO\_malloc(), CRYPTO\_zalloc(),  
CRYPTO\_realloc(), CRYPTO\_clear\_realloc(), OPENSSL\_strdup(), and  
OPENSSL\_strdup() return a pointer to allocated memory or NULL on  
error.

CRYPTO\_set\_mem\_functions() returns 1 on success or 0 on failure (almost  
always because allocations have already happened).

CRYPTO\_mem\_leaks(), CRYPTO\_mem\_leaks\_fp(), CRYPTO\_mem\_leaks\_cb(),  
CRYPTO\_set\_mem\_debug(), and CRYPTO\_mem\_ctrl() are deprecated and are  
no-ops that always return -1. OPENSSL\_mem\_debug\_push(),  
OPENSSL\_mem\_debug\_pop(), CRYPTO\_mem\_debug\_push(), and  
CRYPTO\_mem\_debug\_pop() are deprecated and are no-ops that always return  
0.

## HISTORY

OPENSSL\_mem\_debug\_push(), OPENSSL\_mem\_debug\_pop(),  
CRYPTO\_mem\_debug\_push(), CRYPTO\_mem\_debug\_pop(), CRYPTO\_mem\_leaks(),  
CRYPTO\_mem\_leaks\_fp(), CRYPTO\_mem\_leaks\_cb(), CRYPTO\_set\_mem\_debug(),  
CRYPTO\_mem\_ctrl() were deprecated in OpenSSL 3.0. The memory-leak  
checking has been deprecated in OpenSSL 3.0 in favor of clang's memory  
and leak sanitizer.

Copyright 2016-2022 The OpenSSL Project Authors. All Rights Reserved.  
Licensed under the Apache License 2.0 (the "License"). You may not use  
this file except in compliance with the License. You can obtain a copy  
in the file LICENSE in the source distribution or at  
<<https://www.openssl.org/source/license.html>>.

3.0.7                    2023-07-13            OPENSSSL\_MALLOC(3ossl)