

HEADS UP: OpenSSL problems after GCC 4.2 upgrade

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2007-05/msg00650.html>

- *From:* Alexander Kabaev <kabaev@xxxxxxxxx>
 - *Date:* Sun, 20 May 2007 02:27:22 -0400
-

Hi all,

there were several reports of OpenSSL being broken when compiled with GCC 4.2. It turns out OpenSSL uses function casting feature that was aggressively de-supported by GCC 4.2 and GCC goes as far as inserting invalid instructions ON PURPOSE to discourage the practice.

Consequently, OpenSSL need the patch similar to attached one to work. Just in case mailing list will eat the attachment, the patch can be found at

<http://people.freebsd.org/~kan/openssl-gcc42.diff>

Unfortunately, our OpenSSL maintainer(s) are currently en-route from BSDCan and cannot attend to the matters. Once we figure the best way to fix the code and to integrate the fix into OpenSSL, we will check the fix into CVS. People are advised to patch their sources locally until then.

--

Alexander Kabaev

Index: openssl/crypto/asn1/asn1.h

=====
RCS file: /home/ncvs/src/crypto/openssl/crypto/asn1/asn1.h,v

retrieving revision 1.1.1.8

diff -u -r1.1.1.8 asn1.h

--- openssl/crypto/asn1/asn1.h 29 Jul 2006 19:10:16 -0000 1.1.1.8

+++ openssl/crypto/asn1/asn1.h 20 May 2007 05:01:40 -0000

@@ -903,22 +903,22 @@

/* Used to implement other functions */

void *ASN1_dup(i2d_of_void *i2d, d2i_of_void *d2i, char *x);

#define ASN1_dup_of(type,i2d,d2i,x) \

- ((type (*)(I2D_OF(type),D2I_OF(type),type *))openssl_fcst(ASN1_dup))(i2d,d2i,x)

+ ((type *)ASN1_dup((i2d_of_void *)i2d, (d2i_of_void *)d2i, (char *)x))

#define ASN1_dup_of_const(type,i2d,d2i,x) \

- ((type (*)(I2D_OF_const(type),D2I_OF(type),type *))openssl_fcst(ASN1_dup))(i2d,d2i,x)

+ ((type *)ASN1_dup((i2d_of_void *)i2d, (d2i_of_void *)d2i, (char *)x))

HEADS UP: OpenSSL problems after GCC 4.2 upgrade

```
void *ASN1_item_dup(const ASN1_ITEM *it, void *x);

#ifdef OPENSSSL_NO_FP_API
void *ASN1_d2i_fp(void *(*xnew)(void), d2i_of_void *d2i, FILE *in, void **x);
#define ASN1_d2i_fp_of(type,xnew,d2i,in,x) \
- ((type *(*)(type *(*) (void),D2I_OF(type),FILE *,type **))openssl_fcst(ASN1_d2i_fp))(xnew,d2i,in,x)
+ ((type *)ASN1_d2i_fp((void *(*)(void))(xnew), (d2i_of_void *) (d2i), (in), (void **) (x)))
void *ASN1_item_d2i_fp(const ASN1_ITEM *it, FILE *in, void *x);
int ASN1_i2d_fp(i2d_of_void *i2d,FILE *out,void *x);
#define ASN1_i2d_fp_of(type,i2d,out,x) \
- ((int (*)(I2D_OF(type),FILE *,type *))openssl_fcst(ASN1_i2d_fp))(i2d,out,x)
+ (ASN1_i2d_fp((i2d_of_void *) (i2d), (out), (x)))
#define ASN1_i2d_fp_of_const(type,i2d,out,x) \
- ((int (*)(I2D_OF_const(type),FILE *,type *))openssl_fcst(ASN1_i2d_fp))(i2d,out,x)
+ (ASN1_i2d_fp((i2d_of_void *) (i2d), (out), (x)))
int ASN1_item_i2d_fp(const ASN1_ITEM *it, FILE *out, void *x);
int ASN1_STRING_print_ex_fp(FILE *fp, ASN1_STRING *str, unsigned long flags);
#endif
@@ -928,13 +928,13 @@
#ifdef OPENSSSL_NO_BIO
void *ASN1_d2i_bio(void *(*xnew)(void), d2i_of_void *d2i, BIO *in, void **x);
#define ASN1_d2i_bio_of(type,xnew,d2i,in,x) \
- ((type *(*)(type *(*) (void),D2I_OF(type),BIO *,type **))openssl_fcst(ASN1_d2i_bio))(xnew,d2i,in,x)
+ ((type *)ASN1_d2i_bio( (void *(*)(void))(xnew), (d2i_of_void *) (d2i), (in), (void **) (x)))
void *ASN1_item_d2i_bio(const ASN1_ITEM *it, BIO *in, void *x);
int ASN1_i2d_bio(i2d_of_void *i2d,BIO *out, unsigned char *x);
#define ASN1_i2d_bio_of(type,i2d,out,x) \
- ((int (*)(I2D_OF(type),BIO *,type *))openssl_fcst(ASN1_i2d_bio))(i2d,out,x)
+ (ASN1_i2d_bio((i2d_of_void *) (i2d), (out), (void *) (x)))
#define ASN1_i2d_bio_of_const(type,i2d,out,x) \
- ((int (*)(I2D_OF_const(type),BIO *,const type *))openssl_fcst(ASN1_i2d_bio))(i2d,out,x)
+ (ASN1_i2d_bio((i2d_of_void *) (i2d), (out), (void *) (x)))
int ASN1_item_i2d_bio(const ASN1_ITEM *it, BIO *out, void *x);
int ASN1_UTCTIME_print(BIO *fp,ASN1_UTCTIME *a);
int ASN1_GENERALIZEDTIME_print(BIO *fp,ASN1_GENERALIZEDTIME *a);
@@ -978,7 +978,7 @@
ASN1_STRING *ASN1_pack_string(void *obj, i2d_of_void *i2d,
ASN1_OCTET_STRING **oct);
#define ASN1_pack_string_of(type,obj,i2d,oct) \
- ((ASN1_STRING *(*)(type *,I2D_OF(type),ASN1_OCTET_STRING
**))openssl_fcst(ASN1_pack_string))(obj,i2d,oct)
+ (ASN1_pack_string((obj), (i2d_of_void *) (i2d), (oct)))
ASN1_STRING *ASN1_item_pack(void *obj, const ASN1_ITEM *it, ASN1_OCTET_STRING **oct);

void ASN1_STRING_set_default_mask(unsigned long mask);
Index: openssl/crypto/ocsp/ocsp.h
=====
RCS file: /home/ncvs/src/crypto/openssl/crypto/ocsp/ocsp.h,v
retrieving revision 1.1.1.2
diff -u -r1.1.1.2 ocsp.h
--- openssl/crypto/ocsp/ocsp.h 29 Jul 2006 19:10:18 -0000 1.1.1.2
```

HEADS UP: OpenSSL problems after GCC 4.2 upgrade

```
+++ openssl/crypto/ocsp/ocsp.h 20 May 2007 05:13:06 -0000
@@ -469,7 +469,7 @@
ASN1_STRING *ASN1_STRING_encode(ASN1_STRING *s, i2d_of_void *i2d,
void *data, STACK_OF(ASN1_OBJECT) *sk);
#define ASN1_STRING_encode_of(type,s,i2d,data,sk) \
-((ASN1_STRING *(*)(ASN1_STRING *,I2D_OF(type),type *,STACK_OF(ASN1_OBJECT)
*))openssl_fcast(ASN1_STRING_encode))(s,i2d,data,sk)
+(ASN1_STRING_encode((s), (i2d_of_void *)i2d), (data), (STACK_OF(ASN1_OBJECT) *)sk))

X509_EXTENSION *OCSP_crlID_new(char *url, long *n, char *tim);
```

Index: openssl/crypto/pem/pem.h

```
=====
RCS file: /home/ncvs/src/crypto/openssl/crypto/pem/pem.h,v
retrieving revision 1.1.1.7
diff -u -r1.1.1.7 pem.h
--- openssl/crypto/pem/pem.h 15 Mar 2007 20:03:01 -0000 1.1.1.7
+++ openssl/crypto/pem/pem.h 20 May 2007 06:02:41 -0000
@@ -220,19 +220,20 @@
#define IMPLEMENT_PEM_read_fp(name, type, str, asn1) \
type *PEM_read_##name(FILE *fp, type **x, pem_password_cb *cb, void *u)\
{ \
-return(((type (*)(D2I_OF(type),char *,FILE *,type **,pem_password_cb *,void
*))openssl_fcast(PEM_ASN1_read))(d2i_##asn1, str,fp,x,cb,u)); \
-}
+return((type *)PEM_ASN1_read( \
+ (d2i_of_void *)d2i_##asn1,str,fp,(void **)x,cb,u)); \
+}

#define IMPLEMENT_PEM_write_fp(name, type, str, asn1) \
int PEM_write_##name(FILE *fp, type *x) \
{ \
-return(((int (*)(I2D_OF(type),const char *,FILE *,type *, const EVP_CIPHER *,unsigned char *,int,
pem_password_cb *,void
*))openssl_fcast(PEM_ASN1_write))(i2d_##asn1,str,fp,x,NULL,NULL,0,NULL,NULL)); \
+return(PEM_ASN1_write((i2d_of_void *)i2d_##asn1,str,fp,(char *)x,NULL,NULL,0,NULL,NULL)); \
}

#define IMPLEMENT_PEM_write_fp_const(name, type, str, asn1) \
int PEM_write_##name(FILE *fp, const type *x) \
{ \
-return(((int (*)(I2D_OF_const(type),const char *,FILE *, const type *, const EVP_CIPHER *,unsigned char
*,int, pem_password_cb *,void
*))openssl_fcast(PEM_ASN1_write))(i2d_##asn1,str,fp,x,NULL,NULL,0,NULL,NULL)); \
+return(PEM_ASN1_write((i2d_of_void *)i2d_##asn1,str,fp,(char *)x,NULL,NULL,0,NULL,NULL)); \
}

#define IMPLEMENT_PEM_write_cb_fp(name, type, str, asn1) \
@@ -240,7 +241,7 @@
unsigned char *kstr, int klen, pem_password_cb *cb, \
void *u) \
```

HEADS UP: OpenSSL problems after GCC 4.2 upgrade

```
{ \
- return(((int (*)(I2D_OF(type),const char *,FILE *,type *, const EVP_CIPHER *,unsigned char *,int,
pem_password_cb *,void *))openssl_fcast(PEM_ASN1_write))(i2d_##asn1,str,fp,x,enc,kstr,klen,cb,u)); \
+return(PEM_ASN1_write((i2d_of_void *)i2d_##asn1,str,fp,(char *)x,enc,kstr,klen,cb,u)); \
}

#define IMPLEMENT_PEM_write_cb_fp_const(name, type, str, asn1) \
@@ -248,7 +249,7 @@
unsigned char *kstr, int klen, pem_password_cb *cb, \
void *u) \
{ \
- return(((int (*)(I2D_OF_const(type),const char *,FILE *,type *, const EVP_CIPHER *,unsigned char *,int,
pem_password_cb *,void *))openssl_fcast(PEM_ASN1_write))(i2d_##asn1,str,fp,x,enc,kstr,klen,cb,u)); \
+return(PEM_ASN1_write((i2d_of_void *)i2d_##asn1,str,fp,(char *)x,enc,kstr,klen,cb,u)); \
}

#endif
@@ -256,33 +257,34 @@
#define IMPLEMENT_PEM_read_bio(name, type, str, asn1) \
type *PEM_read_bio_##name(BIO *bp, type **x, pem_password_cb *cb, void *u)\
{ \
- return(((type (*)(D2I_OF(type),const char *,BIO *,type **,pem_password_cb *,void
*))openssl_fcast(PEM_ASN1_read_bio))(d2i_##asn1, str,bp,x,cb,u)); \
+return((type *)PEM_ASN1_read_bio(\
+ (d2i_of_void *)d2i_##asn1,str,bp,(void **)x,cb,u)); \
}

#define IMPLEMENT_PEM_write_bio(name, type, str, asn1) \
int PEM_write_bio_##name(BIO *bp, type *x) \
{ \
- return(((int (*)(I2D_OF(type),const char *,BIO *,type *, const EVP_CIPHER *,unsigned char *,int,
pem_password_cb *,void
*))openssl_fcast(PEM_ASN1_write_bio))(i2d_##asn1,str,bp,x,NULL,NULL,0,NULL,NULL)); \
+return(PEM_ASN1_write_bio((i2d_of_void *)i2d_##asn1,str,bp,(char *)x,NULL,NULL,0,NULL,NULL)); \
}

#define IMPLEMENT_PEM_write_bio_const(name, type, str, asn1) \
int PEM_write_bio_##name(BIO *bp, const type *x) \
{ \
- return(((int (*)(I2D_OF_const(type),const char *,BIO *,const type *, const EVP_CIPHER *,unsigned char
*,int, pem_password_cb *,void
*))openssl_fcast(PEM_ASN1_write_bio))(i2d_##asn1,str,bp,x,NULL,NULL,0,NULL,NULL)); \
+return(PEM_ASN1_write_bio((i2d_of_void *)i2d_##asn1,str,bp,(char *)x,NULL,NULL,0,NULL,NULL)); \
}

#define IMPLEMENT_PEM_write_cb_bio(name, type, str, asn1) \
int PEM_write_bio_##name(BIO *bp, type *x, const EVP_CIPHER *enc, \
unsigned char *kstr, int klen, pem_password_cb *cb, void *u) \
{ \
- return(((int (*)(I2D_OF(type),const char *,BIO *,type *,const EVP_CIPHER *,unsigned char
*,int,pem_password_cb *,void

```

HEADS UP: OpenSSL problems after GCC 4.2 upgrade

```
*)openssl_fcast(PEM_ASN1_write_bio))(i2d_##asn1,str,bp,x,enc,kstr,klen,cb,u)); \
+return(PEM_ASN1_write_bio((i2d_of_void *)i2d_##asn1,str,bp,(char *)x,enc,kstr,klen,cb,u)); \
}

#define IMPLEMENT_PEM_write_cb_bio_const(name, type, str, asn1) \
int PEM_write_bio_##name(BIO *bp, type *x, const EVP_CIPHER *enc, \
unsigned char *kstr, int klen, pem_password_cb *cb, void *u) \
{ \
- return(((int (*)(I2D_OF_const(type),const char *,BIO *,type *,const EVP_CIPHER *,unsigned char \
*,int,pem_password_cb *,void \
*))openssl_fcast(PEM_ASN1_write_bio))(i2d_##asn1,str,bp,x,enc,kstr,klen,cb,u)); \
+return(PEM_ASN1_write_bio((i2d_of_void *)i2d_##asn1,str,bp,(char *)x,enc,kstr,klen,cb,u)); \
}

#define IMPLEMENT_PEM_write(name, type, str, asn1) \
@@ -546,12 +548,12 @@
void * PEM_ASN1_read_bio(d2i_of_void *d2i, const char *name, BIO *bp,
void **x, pem_password_cb *cb, void *u);
#define PEM_ASN1_read_bio_of(type,d2i,name,bp,x,cb,u) \
-((type (*)(D2I_OF(type),const char *,BIO *,type **,pem_password_cb *,void \
*))openssl_fcast(PEM_ASN1_read_bio))(d2i,name,bp,x,cb,u)
+((type *)PEM_ASN1_read_bio((d2i_of_void *)d2i,name,bp,(void **)x,cb,u))
int PEM_ASN1_write_bio(i2d_of_void *i2d,const char *name,BIO *bp,char *x,
const EVP_CIPHER *enc,unsigned char *kstr,int klen,
pem_password_cb *cb, void *u);
#define PEM_ASN1_write_bio_of(type,i2d,name,bp,x,enc,kstr,klen,cb,u) \
- ((int (*)(I2D_OF(type),const char *,BIO *,type *, const EVP_CIPHER *,unsigned char *,int, \
pem_password_cb *,void *))openssl_fcast(PEM_ASN1_write_bio))(i2d,name,bp,x,enc,kstr,klen,cb,u)
+ (PEM_ASN1_write_bio)((i2d_of_void *)i2d,name,bp,(char *)x,enc,kstr,klen,cb,u)

STACK_OF(X509_INFO) * PEM_X509_INFO_read_bio(BIO *bp, STACK_OF(X509_INFO) *sk,
pem_password_cb *cb, void *u);
int PEM_X509_INFO_write_bio(BIO *bp,X509_INFO *xi, EVP_CIPHER *enc,
```

Attachment: [signature.asc](#)

Description: PGP signature