**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 349 - C:\Users\Jeremy\Downloads\crypto.c

Don't know how to do that \*/

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 367 - C:\Users\Jeremy\Downloads\crypto.c

Don't know how to do that \*/

**STANDARD: Potentially Unsafe Code - strlen**

Line: 400 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

unsigned name\_sz = strlen(libname);

**STANDARD: Potentially Unsafe Code - strlen**

Line: 402 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

unsigned ver\_sz = strlen(ver);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 405 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(enif\_make\_new\_binary(env, name\_sz, &name\_term), libname, name\_sz);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 406 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(enif\_make\_new\_binary(env, ver\_sz, &ver\_term), ver, ver\_sz);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 442 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(new\_ctx, ctx\_bin.data, MD5\_CTX\_LEN);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 454 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(&ctx\_clone, ctx\_bin.data, MD5\_CTX\_LEN);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 487 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(new\_ctx, ctx\_bin.data, SHA\_CTX\_LEN);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 499 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(&ctx\_clone, ctx\_bin.data, SHA\_CTX\_LEN);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 532 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(new\_ctx, ctx\_bin.data, MD4\_CTX\_LEN);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 544 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(&ctx\_clone, ctx\_bin.data, MD4\_CTX\_LEN);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 562 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(enif\_make\_new\_binary(env, mac\_sz, &ret), hmacbuf, mac\_sz);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 579 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(enif\_make\_new\_binary(env, mac\_sz, &ret),

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 597 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(&ivec\_clone, ivec.data, 8);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 636 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(&ivec\_clone, ivec.data, 8);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 661 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(ivec\_clone, ivec.data, 16);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 687 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(ivec\_clone, ivec.data, 16);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 693 - C:\Users\Jeremy\Downloads\crypto.c

To do an incremental {en|de}cryption, the state to to keep between calls

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 900 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(hmacbuf, data\_bin.data, SHA\_DIGEST\_LENGTH);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 903 - C:\Users\Jeremy\Downloads\crypto.c

Use of 'goto' function. The goto function can result in unstructured code which is difficult to maintain and can result in failures to initialise or de-allocate memory.

goto badarg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 928 - C:\Users\Jeremy\Downloads\crypto.c

Use of 'goto' function. The goto function can result in unstructured code which is difficult to maintain and can result in failures to initialise or de-allocate memory.

else goto badarg;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 986 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(ivec, ivec\_bin.data, 16);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1053 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(rc4\_key, state.data, sizeof(RC4\_KEY));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 1096 - C:\Users\Jeremy\Downloads\crypto.c

Use of 'goto' function. The goto function can result in unstructured code which is difficult to maintain and can result in failures to initialise or de-allocate memory.

else goto badarg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 1157 - C:\Users\Jeremy\Downloads\crypto.c

Use of 'goto' function. The goto function can result in unstructured code which is difficult to maintain and can result in failures to initialise or de-allocate memory.

goto badarg;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1164 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(hmacbuf, data\_bin.data, SHA\_DIGEST\_LENGTH);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1451 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(bf\_tkey, ivec\_bin.data, 8);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1474 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(bf\_tkey, ivec\_bin.data, 8);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1514 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(bf\_tkey, ivec\_bin.data, 8);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1596 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(ipad, key, klen);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1597 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(opad, key, klen);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1635 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(ipad, key, klen);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 1636 - C:\Users\Jeremy\Downloads\crypto.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions and other memory mis-management situations.

memcpy(opad, key, klen);

**STANDARD: Potential Memory Mis-management. Variable Name: bn\_rand**

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 826 FileName: C:\Users\Jeremy\Downloads\crypto.c

**STANDARD: Potential Memory Mis-management. Variable Name: bn\_from**

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 826 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 827 FileName: C:\Users\Jeremy\Downloads\crypto.c

**STANDARD: Potential Memory Mis-management. Variable Name: bn\_base**

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 826 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 827 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 859 FileName: C:\Users\Jeremy\Downloads\crypto.c

**STANDARD: Potential Memory Mis-management. Variable Name: bn\_exponent**

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 826 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 827 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 859 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 858 FileName: C:\Users\Jeremy\Downloads\crypto.c

**STANDARD: Potential Memory Mis-management. Variable Name: dsa**

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 826 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 827 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 859 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 858 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 1175 FileName: C:\Users\Jeremy\Downloads\crypto.c

**STANDARD: Potential Memory Mis-management. Variable Name: rsa**

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 826 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 827 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 859 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 858 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 1175 FileName: C:\Users\Jeremy\Downloads\crypto.c

2 free

Multiple frees detected. Check code paths manually to ensure that variables cannot be freed more than once.

Line: 1290 FileName: C:\Users\Jeremy\Downloads\crypto.c