**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 48 - C:\Users\Jeremy\Downloads\shash.c

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

memcpy(alignbuffer, key, keylen);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 89 - C:\Users\Jeremy\Downloads\shash.c

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

memcpy(buf, data, unaligned\_len);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 124 - C:\Users\Jeremy\Downloads\shash.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 out;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 126 - C:\Users\Jeremy\Downloads\shash.c

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

memcpy(out, buf, ds);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 190 - C:\Users\Jeremy\Downloads\shash.c

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

memcpy(out, shash\_desc\_ctx(desc), crypto\_shash\_descsize(desc->tfm));

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 196 - C:\Users\Jeremy\Downloads\shash.c

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

memcpy(shash\_desc\_ctx(desc), in, crypto\_shash\_descsize(desc->tfm));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 427 - C:\Users\Jeremy\Downloads\shash.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 432 - C:\Users\Jeremy\Downloads\shash.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 436 - C:\Users\Jeremy\Downloads\shash.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 out;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 533 - C:\Users\Jeremy\Downloads\shash.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rhash.type, "shash", sizeof(rhash.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 533 - C:\Users\Jeremy\Downloads\shash.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rhash.type, "shash", sizeof(rhash.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 540 - C:\Users\Jeremy\Downloads\shash.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 640 - C:\Users\Jeremy\Downloads\shash.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 err;

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

malloc without free.

Line: 471 FileName: C:\Users\Jeremy\Downloads\shash.c

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 68 - C:\Users\Jeremy\Downloads\rng.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rrng.type, "rng", sizeof(rrng.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 68 - C:\Users\Jeremy\Downloads\rng.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rrng.type, "rng", sizeof(rrng.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 74 - C:\Users\Jeremy\Downloads\rng.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 121 - C:\Users\Jeremy\Downloads\rng.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 unlock;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 126 - C:\Users\Jeremy\Downloads\rng.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 unlock;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 56 - C:\Users\Jeremy\Downloads\pcompress.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rpcomp.type, "pcomp", sizeof(rpcomp.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 56 - C:\Users\Jeremy\Downloads\pcompress.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rpcomp.type, "pcomp", sizeof(rpcomp.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 59 - C:\Users\Jeremy\Downloads\pcompress.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 nla\_put\_failure;

**STANDARD: Potentially Unsafe Code - strlen**

Line: 57 - C:\Users\Jeremy\Downloads\crypto\_user.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.

if (strlen(p->cru\_driver\_name))

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 78 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rcipher.type, "cipher", sizeof(rcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 78 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rcipher.type, "cipher", sizeof(rcipher.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 86 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 97 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rcomp.type, "compression", sizeof(rcomp.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 97 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rcomp.type, "compression", sizeof(rcomp.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 100 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 110 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(ualg->cru\_name, alg->cra\_name, sizeof(ualg->cru\_name));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 110 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(ualg->cru\_name, alg->cra\_name, sizeof(ualg->cru\_name));

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 111 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(ualg->cru\_driver\_name, alg->cra\_driver\_name,

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 111 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(ualg->cru\_driver\_name, alg->cra\_driver\_name,

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 113 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(ualg->cru\_module\_name, module\_name(alg->cra\_module),

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 113 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(ualg->cru\_module\_name, module\_name(alg->cra\_module),

**MEDIUM: Potentially Unsafe Code - goto**

Line: 122 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 126 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rl.type, "larval", sizeof(rl.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 126 - C:\Users\Jeremy\Downloads\crypto\_user.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rl.type, "larval", sizeof(rl.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 129 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 130 - C:\Users\Jeremy\Downloads\crypto\_user.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 135 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 137 - C:\Users\Jeremy\Downloads\crypto\_user.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 143 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 148 - C:\Users\Jeremy\Downloads\crypto\_user.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 173 - C:\Users\Jeremy\Downloads\crypto\_user.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 181 - C:\Users\Jeremy\Downloads\crypto\_user.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 229 - C:\Users\Jeremy\Downloads\crypto\_user.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 241 - C:\Users\Jeremy\Downloads\crypto\_user.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 out\_err;

**STANDARD: Potentially Unsafe Code - strlen**

Line: 263 - C:\Users\Jeremy\Downloads\crypto\_user.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.

if (priority && !strlen(p->cru\_driver\_name))

**STANDARD: Potentially Unsafe Code - strlen**

Line: 371 - C:\Users\Jeremy\Downloads\crypto\_user.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.

if (strlen(p->cru\_driver\_name))

**STANDARD: Potentially Unsafe Code - strlen**

Line: 381 - C:\Users\Jeremy\Downloads\crypto\_user.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.

if (strlen(p->cru\_driver\_name))

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

new without delete.

Line: 206 FileName: C:\Users\Jeremy\Downloads\crypto\_user.c

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 91 - C:\Users\Jeremy\Downloads\blkcipher.c

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

memcpy(walk->dst.virt.addr, walk->page, n);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 118 - C:\Users\Jeremy\Downloads\blkcipher.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 err;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 139 - C:\Users\Jeremy\Downloads\blkcipher.c

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

memcpy(desc->info, walk->iv, crypto\_blkcipher\_ivsize(tfm));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 158 - C:\Users\Jeremy\Downloads\blkcipher.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 ok;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 162 - C:\Users\Jeremy\Downloads\blkcipher.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 ok;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 190 - C:\Users\Jeremy\Downloads\blkcipher.c

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

memcpy(tmp, walk->src.virt.addr, walk->nbytes);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 259 - C:\Users\Jeremy\Downloads\blkcipher.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 set\_phys\_lowmem;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 265 - C:\Users\Jeremy\Downloads\blkcipher.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 set\_phys\_lowmem;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 301 - C:\Users\Jeremy\Downloads\blkcipher.c

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

walk->iv = memcpy(iv, walk->iv, ivsize);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 376 - C:\Users\Jeremy\Downloads\blkcipher.c

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

memcpy(alignbuffer, key, keylen);

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 502 - C:\Users\Jeremy\Downloads\blkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.type, "blkcipher", sizeof(rblkcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 502 - C:\Users\Jeremy\Downloads\blkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.type, "blkcipher", sizeof(rblkcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 503 - C:\Users\Jeremy\Downloads\blkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.geniv, alg->cra\_blkcipher.geniv ?: "<default>",

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 503 - C:\Users\Jeremy\Downloads\blkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.geniv, alg->cra\_blkcipher.geniv ?: "<default>",

**MEDIUM: Potentially Unsafe Code - goto**

Line: 513 - C:\Users\Jeremy\Downloads\blkcipher.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 614 - C:\Users\Jeremy\Downloads\blkcipher.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 err\_free\_inst;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 643 - C:\Users\Jeremy\Downloads\blkcipher.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 655 - C:\Users\Jeremy\Downloads\blkcipher.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 657 - C:\Users\Jeremy\Downloads\blkcipher.c

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

memcpy(inst->alg.cra\_name, alg->cra\_name, CRYPTO\_MAX\_ALG\_NAME);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 658 - C:\Users\Jeremy\Downloads\blkcipher.c

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

memcpy(inst->alg.cra\_driver\_name, alg->cra\_driver\_name,

**MEDIUM: Potentially Unsafe Code - goto**

Line: 665 - C:\Users\Jeremy\Downloads\blkcipher.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 669 - C:\Users\Jeremy\Downloads\blkcipher.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 696 - C:\Users\Jeremy\Downloads\blkcipher.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 out;

**STANDARD: Potential Memory Mis-management. Variable Name: walk->buffer**

malloc without free.

Line: 292 FileName: C:\Users\Jeremy\Downloads\blkcipher.c

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

malloc without free.

Line: 292 FileName: C:\Users\Jeremy\Downloads\blkcipher.c

2 free

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

Line: 703 FileName: C:\Users\Jeremy\Downloads\blkcipher.c

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 163 - C:\Users\Jeremy\Downloads\ahash.c

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

memcpy(alignbuffer, key, keylen);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 201 - C:\Users\Jeremy\Downloads\ahash.c

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

memcpy(priv->result, req->result,

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 287 - C:\Users\Jeremy\Downloads\ahash.c

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

memcpy(priv->result, req->result,

**MEDIUM: Potentially Unsafe Code - goto**

Line: 308 - C:\Users\Jeremy\Downloads\ahash.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 out;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 407 - C:\Users\Jeremy\Downloads\ahash.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rhash.type, "ahash", sizeof(rhash.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 407 - C:\Users\Jeremy\Downloads\ahash.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rhash.type, "ahash", sizeof(rhash.type));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 414 - C:\Users\Jeremy\Downloads\ahash.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 nla\_put\_failure;

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

malloc without free.

Line: 338 FileName: C:\Users\Jeremy\Downloads\ahash.c

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 44 - C:\Users\Jeremy\Downloads\aead.c

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

memcpy(alignbuffer, key, keylen);

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 120 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.type, "aead", sizeof(raead.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 120 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.type, "aead", sizeof(raead.type));

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 121 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.geniv, aead->geniv ?: "<built-in>", sizeof(raead.geniv));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 121 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.geniv, aead->geniv ?: "<built-in>", sizeof(raead.geniv));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 129 - C:\Users\Jeremy\Downloads\aead.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 nla\_put\_failure;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 205 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.type, "nivaead", sizeof(raead.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 205 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.type, "nivaead", sizeof(raead.type));

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 206 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.geniv, aead->geniv, sizeof(raead.geniv));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 206 - C:\Users\Jeremy\Downloads\aead.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(raead.geniv, aead->geniv, sizeof(raead.geniv));

**MEDIUM: Potentially Unsafe Code - goto**

Line: 214 - C:\Users\Jeremy\Downloads\aead.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 307 - C:\Users\Jeremy\Downloads\aead.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 err\_free\_inst;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 313 - C:\Users\Jeremy\Downloads\aead.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 322 - C:\Users\Jeremy\Downloads\aead.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 324 - C:\Users\Jeremy\Downloads\aead.c

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

memcpy(inst->alg.cra\_name, alg->cra\_name, CRYPTO\_MAX\_ALG\_NAME);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 325 - C:\Users\Jeremy\Downloads\aead.c

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

memcpy(inst->alg.cra\_driver\_name, alg->cra\_driver\_name,

**MEDIUM: Potentially Unsafe Code - goto**

Line: 332 - C:\Users\Jeremy\Downloads\aead.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 336 - C:\Users\Jeremy\Downloads\aead.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 err\_drop\_alg;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 363 - C:\Users\Jeremy\Downloads\aead.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 418 - C:\Users\Jeremy\Downloads\aead.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 422 - C:\Users\Jeremy\Downloads\aead.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 drop\_larval;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 434 - C:\Users\Jeremy\Downloads\aead.c

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

memcpy(palg.data.name, alg->cra\_driver\_name, CRYPTO\_MAX\_ALG\_NAME);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 444 - C:\Users\Jeremy\Downloads\aead.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 kill\_larval;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 449 - C:\Users\Jeremy\Downloads\aead.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 put\_tmpl;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 453 - C:\Users\Jeremy\Downloads\aead.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 put\_tmpl;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 541 - C:\Users\Jeremy\Downloads\aead.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 err;

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

3 free

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

Line: 452 FileName: C:\Users\Jeremy\Downloads\aead.c

**MEDIUM: Potentially Unsafe Code - goto**

Line: 124 - C:\Users\Jeremy\Downloads\ablkcipher.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 err;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 145 - C:\Users\Jeremy\Downloads\ablkcipher.c

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

memcpy(req->info, walk->iv, tfm->crt\_ablkcipher.ivsize);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 213 - C:\Users\Jeremy\Downloads\ablkcipher.c

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

walk->iv = memcpy(iv, walk->iv, ivsize);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 255 - C:\Users\Jeremy\Downloads\ablkcipher.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 set\_phys\_lowmem;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 324 - C:\Users\Jeremy\Downloads\ablkcipher.c

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

memcpy(alignbuffer, key, keylen);

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 391 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.type, "ablkcipher", sizeof(rblkcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 391 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.type, "ablkcipher", sizeof(rblkcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 392 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.geniv, alg->cra\_ablkcipher.geniv ?: "<default>",

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 392 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.geniv, alg->cra\_ablkcipher.geniv ?: "<default>",

**MEDIUM: Potentially Unsafe Code - goto**

Line: 402 - C:\Users\Jeremy\Downloads\ablkcipher.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 nla\_put\_failure;

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 472 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.type, "givcipher", sizeof(rblkcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 472 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.type, "givcipher", sizeof(rblkcipher.type));

**STANDARD: Potentially Unsafe Code - strncpy**

Line: 473 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.geniv, alg->cra\_ablkcipher.geniv ?: "<built-in>",

**STANDARD: Potentially Unsafe Code - strncpy(**

Line: 473 - C:\Users\Jeremy\Downloads\ablkcipher.c

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions. While 'safer', the current "n" functions include non-null termination of overflowed buffers and no error returns on overflow.

strncpy(rblkcipher.geniv, alg->cra\_ablkcipher.geniv ?: "<built-in>",

**MEDIUM: Potentially Unsafe Code - goto**

Line: 483 - C:\Users\Jeremy\Downloads\ablkcipher.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 nla\_put\_failure;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 557 - C:\Users\Jeremy\Downloads\ablkcipher.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 out;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 561 - C:\Users\Jeremy\Downloads\ablkcipher.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 drop\_larval;

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 573 - C:\Users\Jeremy\Downloads\ablkcipher.c

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

memcpy(palg.data.name, alg->cra\_driver\_name, CRYPTO\_MAX\_ALG\_NAME);

**MEDIUM: Potentially Unsafe Code - goto**

Line: 590 - C:\Users\Jeremy\Downloads\ablkcipher.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 kill\_larval;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 595 - C:\Users\Jeremy\Downloads\ablkcipher.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 put\_tmpl;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 599 - C:\Users\Jeremy\Downloads\ablkcipher.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 put\_tmpl;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 690 - C:\Users\Jeremy\Downloads\ablkcipher.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 err;

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

malloc without free.

Line: 167 FileName: C:\Users\Jeremy\Downloads\ablkcipher.c

**STANDARD: Potential Memory Mis-management. Variable Name: walk->iv\_buffer**

malloc without free.

Line: 167 FileName: C:\Users\Jeremy\Downloads\ablkcipher.c

malloc without free.

Line: 204 FileName: C:\Users\Jeremy\Downloads\ablkcipher.c