**STANDARD: Potential Memory Mis-management. Variable Name: p8inf**

2 free

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

Line: 531 FileName: C:\Users\Jeremy\Downloads\x\_all.c

**MEDIUM: Potentially Unsafe Code - goto**

Line: 97 - C:\Users\Jeremy\Downloads\ecs\_vrf.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.

if (d2i\_ECDSA\_SIG(&s, &p, sig\_len) == NULL) goto err;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 101 - C:\Users\Jeremy\Downloads\ecs\_vrf.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 - goto**

Line: 187 - C:\Users\Jeremy\Downloads\dsa\_asn1.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.

if (d2i\_DSA\_SIG(&s,&p,siglen) == NULL) goto err;

**MEDIUM: Potentially Unsafe Code - goto**

Line: 191 - C:\Users\Jeremy\Downloads\dsa\_asn1.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: sig**

malloc without free.

Line: 72 FileName: C:\Users\Jeremy\Downloads\dsa\_asn1.c

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

malloc without free.

Line: 72 FileName: C:\Users\Jeremy\Downloads\dsa\_asn1.c

new without delete.

Line: 98 FileName: C:\Users\Jeremy\Downloads\dsa\_asn1.c

**MEDIUM: Potentially Unsafe Code - goto**

Line: 91 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 97 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 105 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 120 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 130 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 171 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 178 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 187 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 197 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 204 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 211 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 221 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 232 - C:\Users\Jeremy\Downloads\a\_verify.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 - goto**

Line: 241 - C:\Users\Jeremy\Downloads\a\_verify.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: buf\_in**

2 free

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

Line: 227 FileName: C:\Users\Jeremy\Downloads\a\_verify.c