**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 106 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(key\_s, key.data(), use\_key\_length);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 110 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(key\_s, key.data(), MIN(key.size(), key\_length\_sizes[0]));

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 122 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(key\_s, key.data(), MIN(key.size(), use\_key\_length));

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 138 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(iv\_s, iv.data(), iv\_size);

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 159 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(data\_s, data.data(), data.size());

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 164 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(data\_s, data.data(), data.size());

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 212 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(data\_s, data.data(), data.size());

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 217 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(data\_s, data.data(), data.size());

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 588 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(key\_s, key.data(), key.size());

**MEDIUM: Potentially Unsafe Code - memcpy**

Line: 594 - C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

memcpy(iv\_s, iv.data(), iv\_size);

**STANDARD: Potential Memory Mis-management. Variable Name: key\_sizes**

2 free

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

The use of malloc() and free() functions in C++ code is not recommended and can result in errors that would otherwise have been avoided with new and delete.

Line: 543 FileName: C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

2 free

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

The use of malloc() and free() functions in C++ code is not recommended and can result in errors that would otherwise have been avoided with new and delete.

Line: 543 FileName: C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

2 free

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

The use of malloc() and free() functions in C++ code is not recommended and can result in errors that would otherwise have been avoided with new and delete.

Line: 372 FileName: C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

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

2 free

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

The use of malloc() and free() functions in C++ code is not recommended and can result in errors that would otherwise have been avoided with new and delete.

Line: 543 FileName: C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

2 free

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

The use of malloc() and free() functions in C++ code is not recommended and can result in errors that would otherwise have been avoided with new and delete.

Line: 372 FileName: C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp

2 free

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

The use of malloc() and free() functions in C++ code is not recommended and can result in errors that would otherwise have been avoided with new and delete.

Line: 530 FileName: C:\Users\Jeremy\Downloads\buggy\_ext\_mcrypt.cpp