How do I create a SAL annotation for a structure with a variable-length array?

devblogs.microsoft.com/oldnewthing/20180517-00

May 17, 2018

Raymond Chen

Some Windows structures end with an array of size 1. If you try to access any members of that array beyond the first, you may get a static analysis error.

```
typedef struct THINGGROUP
{
  DWORD NumberOfThings;
  THING Things[ANYSIZE_ARRAY];
};

void ProcessAllTheThings(_In_ const THINGGROUP* group)
{
 for (DWORD index = 0; index < group->NumberOfThings; index++) {
  // static analysis warning: possible index past end of array
  // when NumberOfThings >= 2
  ProcessOneThing(group->Things[index]);
 }
}
```

How do you tell the Visual Studio static analysis tool that the size of the `Things` array is specified by the `NumberOfThings` member?

You use the `_Field_size_` annotation. The documentation doesn't really give an example of this case, so here you go:

```
typedef struct THINGGROUP
{
  DWORD NumberOfThings;
  _Field_size_(NumberOfThings)
  THING Things[ANYSIZE_ARRAY];
};
```

Raymond Chen

Follow