Buffer Overflow

WEAKNESS

ACCESS AND OUT-OF-BOUNDS READ #125, #126, #127, #786
ACCESS AND OUT-OF-BOUNDS WRITE #787, #788, #124

FAILURE TO CONSTRAIN OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER #119

IMPROPER-ACCESS-OF-INDEXABLE-RESOURCE #118

CAN-PRECEDE

RESOURCE/LOCATION

STACK-BASED #121
ARRAY #129
HEAP-BASED #122

MEMORY-BUFFER #119
BUFFER #119
INDEX #466
INDEXABLE-RESOURCE #118

CONSEQUENCES

WRITE-WHAT-WHERE CONDITION #123
UNCONTROLLED MEMORY ALLOCATION #789
INFORMATION LOSS OR OMISSION #199 #221

IMPROPER-ACCESS-OF-INDEXABLE-RESOURCE #118

SIGN ERRORS #194 #195 #196
INCORRECT-BUFFER-SIZE-CALCULATION #131
IMPROPER-INPUT-VALIDATION #20
OFF-BY-ONE #193
INTEGER COERCION ERROR #192
INTEGER OVERFLOW #190 #680
INTEGER UNDERFLOW #191
WRAP-AROUND ERROR #128
POINTER ERRORS #467 #468
IMPROPER HANDLING OF LENGTH PARAMETER INCONSISTENCY # 130
IMPROPER HANDLING OF EXTRA VALUES #231
RETURN OF POINTER VALUE OUTSIDE OF EXPECTED RANGE #466
IMPROPER NULL TERMINATION #170
IMPROPER VALIDATION OF ARRAY INDEX #129 #789
BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') #120

SOFTWARE-FAULT

INTEGER OVERFLOW #190 #680
OVERFLOW

WEAKNESS

ACCESS AND OUT-OF-BOUNDS READ #125, #126, #127, #786
ACCESS AND OUT-OF-BOUNDS WRITE #787, #788, #124

FAILURE TO CONSTRAIN OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER #119

IMPROPER-ACCESS-OF-INDEXABLE-RESOURCE #118

CAN-PRECEDE

RESOURCE/LOCATION

STACK-BASED #121
ARRAY #129
HEAP-BASED #122

MEMORY-BUFFER #119
BUFFER #119
INDEX #466
INDEXABLE-RESOURCE #118

CONSEQUENCES

WRITE-WHAT-WHERE CONDITION #123
UNCONTROLLED MEMORY ALLOCATION #789
INFORMATION LOSS OR OMISSION #199 #221

IMPROPER-ACCESS-OF-INDEXABLE-RESOURCE #118

SIGN ERRORS #194 #195 #196
INCORRECT-BUFFER-SIZE-CALCULATION #131
IMPROPER-INPUT-VALIDATION #20
OFF-BY-ONE #193
INTEGER COERCION ERROR #192
INTEGER OVERFLOW #190 #680
INTEGER UNDERFLOW #191
WRAP-AROUND ERROR #128
POINTER ERRORS #467 #468
IMPROPER HANDLING OF LENGTH PARAMETER INCONSISTENCY # 130
IMPROPER HANDLING OF EXTRA VALUES #231
RETURN OF POINTER VALUE OUTSIDE OF EXPECTED RANGE #466
IMPROPER NULL TERMINATION #170
IMPROPER VALIDATION OF ARRAY INDEX #129 #789
BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') #120

SOFTWARE-FAULT

INTEGER OVERFLOW #190 #680
OVERFLOW