Datasheet

Mayhem Sanitizers

ForAllSecure

Sanitizers add checking capabilities that allow Mayhem to instrument binaries and uncover security defects that may not result in an immediate crash. Mayhem supports ASAN, UBSAN, LSAN, MSAN, Valgrind, and other proprietary checkers, which enable the detection of the following Common Weakness Enumerations (CWEs):

CWE #	Title
20	Improper Input Validation
115	Misinterpretation of Input
119	Improper Restriction of Operations within the Bounds of a Memory Buffer
121	Stack-based Buffer Overflow
122	Heap-based Buffer Overflow
125	Out-of-bounds Read
129	Improper Validation of Array Index
131	Incorrect Calculation of Buffer Size
188	Reliance on Data/Memory Layout
190	Integer Overflow or Wraparound
197	Numeric Truncation Error
233	Improper Handling of Parameters
369	Divide By Zero
393	Return of Wrong Status Code
400	Uncontrolled Resource Consumption
401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')
415	Double Free
416	Use After Free
457	Use of Uninitialized Variable
469	Use of Pointer Subtraction to Determine Size

CWE #	Title
476	NULL Pointer Dereference
561	Dead Code
562	Return of Stack Variable Address
590	Free of Memory not on the Heap
664	Improper Control of a Resource Through its Lifetime
665	Improper Initialization
680	Integer Overflow to Buffer Overflow
690	Unchecked Return Value to NULL Pointer Dereference
704	Incorrect Type Conversion or Cast
758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
763	Release of Invalid Pointer or Reference
786	Access of Memory Location Before Start of Buffer
787	Out-of-bounds Write
788	Access of Memory Location After End of Buffer
789	Uncontrolled Memory Allocation
913	Improper Control of Dynamically-Managed Code Resource