memory safety

Accessing memory typically outside the bounds of a data structure which then provides a vector to attack from to conduct further exploitation/attack.

Android	>65% of High & Critical security bugs
Android (bluetooth & media components)	90% of vulnerabilities
IOS 12	66.3% of all vulnerabilities
MacOS Mojave	71.5% of all vulnerabilities
Chrome	~70% of serious security bugs
Microsoft	~70% of CVE vulnerabilities
Firefox (CSS subsystem)	73.9% of bugs
Ubuntu kernel	65% of CVEs (In security updates between November and May 2020)

(Alex Gaynor, 2020)

Each statistic is that of a large code base containing millions of lines of code.

All are written in C or C++.

Includes;

- Use-after-free
- Double-free
- Heap Buffer overflow
- Integer overflow
- Out-of-bounds read
- Out-of-bounds write

Image: David Carson