Software Security Course 2019/2020

Andrea Lanzi

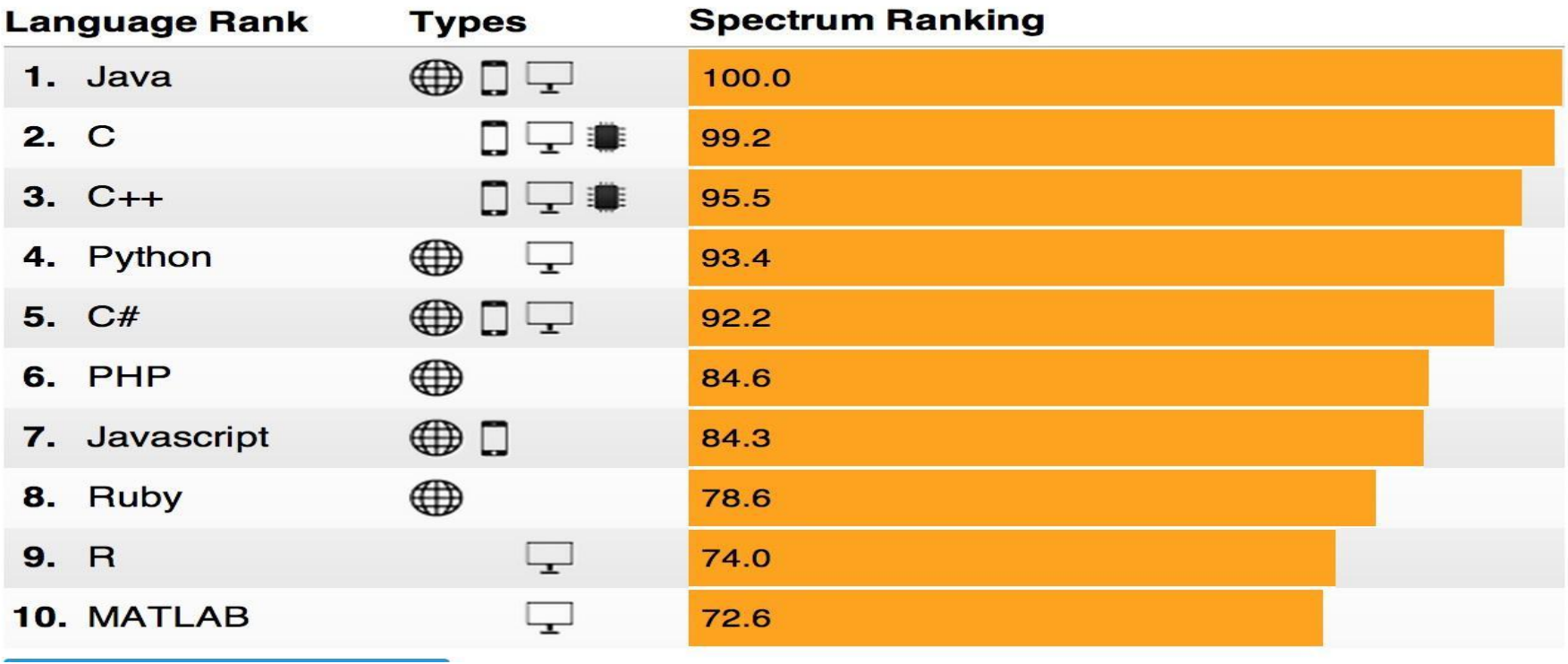
Buffer Overflow

- A buffer overflow is a bug that affects low-level code, typically in C and C++, with significant security implications.
- Normally, a program with this bug will simply crash
- But an attacker can alter the situations that cause the program to do much worse
    - Steal private information (e.g., Heartbleed)
    - Corrupt valuable information
    - Run code of the attacker’s choice

Why there are so important?

- Buffer overflows are still **relevant** today
  - C and C++ are still popular
  - Buffer overflows still occur with regularity
- They have a **long history**
  - Many different approaches developed to defend against them, and bugs like them.
- They share **common features with other bugs** that we will study
  - In **how the attack works**
  - In **how to defend against it**

C and C++ still very popular



Critical systems in C/C++

- Most OS kernels and utilities
  - Fingerd, X windows server, shell
- Many high-performance servers
  - Microsoft IIS, Apache httpd, nginx
  - Microsoft SQL server, MySQL, redis, memcached
- Many embedded systems
  - Mars rover, industrial control systems, automobiles

History of buffer overflows

- **1988 Morris Worm**, Propagated across machines (too aggressively, thanks to a bug)
- One way it propagated was a buffer overflow attack against a vulnerable version of fingerd on VAXes
- Sent a special string to the finger daemon, which caused it to execute code that created a new worm copy
- End result: **$10-100M in damages, probation, community service**

History of buffer overflows

- **2001 Code Red**, Exploited an overflow in the MS-IIS server, 300,000 machines infected in 14 hours.
- **2003 SQL slammer,** Exploited an overflow in the MS-SQL server, 75,000 machines infected in 10 minutes.

Slashdot

stories
submissions
popular
blog

ask slashdot
book reviews
games
idle
yro
technology

23-Year-Old X11 Server Security Vulnerability Discovered

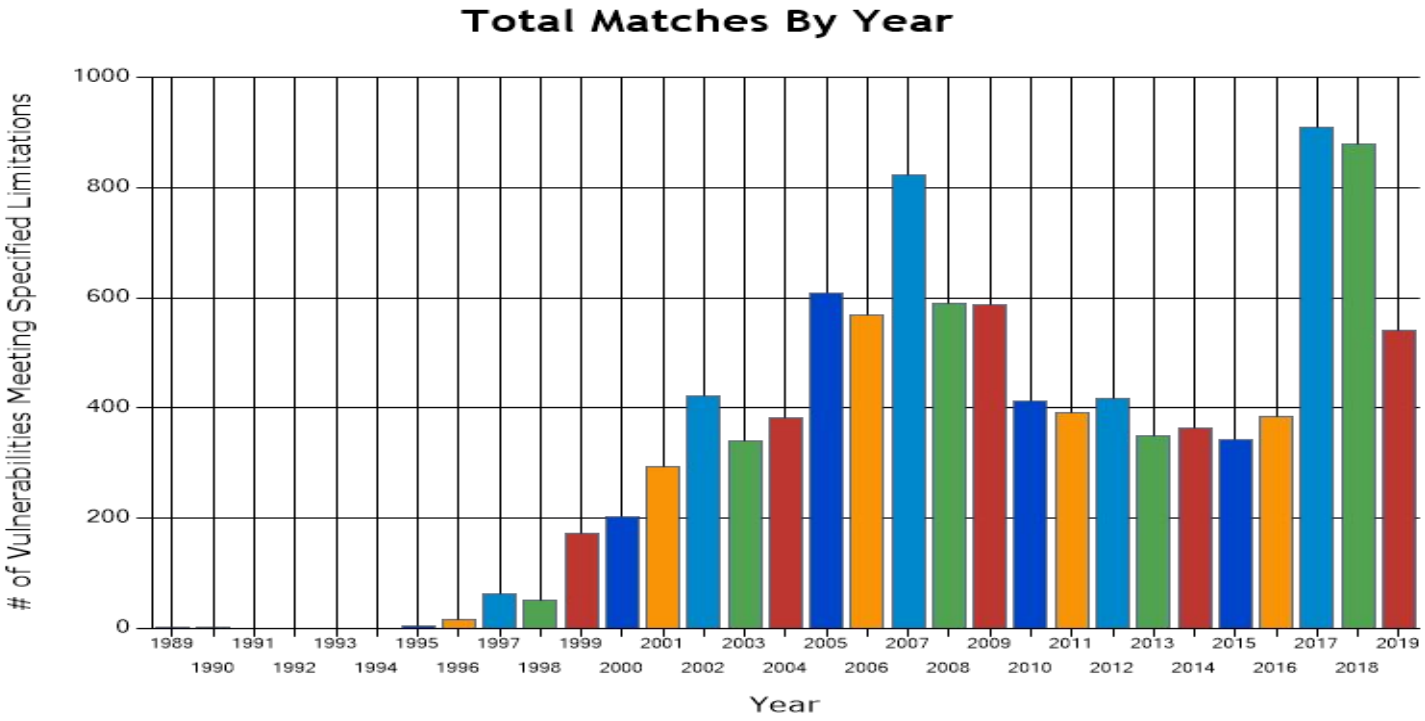
Posted by **Unknown Lamer** on Wednesday January 08, 2014 @10:11
from the stack-smashing-for-fun-and-profit dept.

An anonymous reader writes

> "The recent report of X11/X.Org security in bad shape rings more truth today. The X.Org Foundation announced today that they've found a X11 security issue that dates back to 1991. The issue is a possible stack buffer overflow that could lead to privilege escalation to root and affects all versions of the X Server back to X11R5. After the vulnerability being in the code-base for 23 years, it was finally uncovered via the automated cppcheck static analysis utility."

There's a `scanf` used when loading BDF fonts that can overflow using a carefully crafted font. Watch out for those obsolete early-90s bitmap fonts.

Vulnerability Trend



What we'll do

- Understand how these attacks work, and how to defend against them
- These require knowledge about:
  - The compiler
  - The OS
  - The architecture