William Prado
07/24/2025
Apps/Cloud Vulnerabilities.

windows Library
DLL injection - Microsoft Libraries

- attackers inject a path to a malicious DLL.
- one of the most popularmemory injection method.

Tech SKY YTB

Buffer overflow attacks Explained | How attackers exploits memory.

Scope - evaluation Target.

|| refers to product, system, or service being analyzed for potention security vulnerability.

Cloud Side-channel Attack

Cloud cryptojacking - attacker uses cloud's processing power to mine cryptocurrency.

YTB - CASB 101: Why does anyone need a casb?

CASB = Cloud Access Security Broker

- enable single sign on authentication
- authorization from enterprise Network to CSP
- monitor & audit user and resource activity

3 Implementation methods.

- forward proxy
- reverse proxy
- API

Willian Prado
07/24/2025
web vulnerabilities

YTB → What is an SBOM? Software Bill of Materials

prof. Messer YTB → Application Attack

- Buffer overflow
- Replay attack
- Privilege escalation < • vertide • Horizontal

Mitigating privilege escalation

* patch
  - fix the vulnerability.
* updated anti-virus/anti-malware software
* Data Execution Prevention
* Address space layout

powercert videos YTB _ SSL, TLS, HTTP, HTTPS, explained.

Elevation of privilege vulnerability

Cross-site request

The client + the server

Cross-site request forgery

../.. Directory traversal / path traversal

https://www.amazon.com/home.html?view=../../windows/system

sunny classroom. YTB TCP - 3 way handshake in details

Web vulnerabilities

TCP handshake.

Syn →

SYN ACK

ACK

1. session starting, 2. Convesatio 3. Ending sessing

SYN = synchronize

ACK = Acknowledge / Ackn

2. Data Transmission

3. 4-step procedure to close the session.

sunny classroom YTB How TCP Starts + close session?

William Prado
07/24/2025
Vulnerability types

Legacy systems
End of Life (EOL)/End-of-Service Life (EOSL) systems
Lack of vendor support

*- VM Escape protection • malware code running in VM breaking out + interacting w/ the host OS or other Vms (via hypervisor).

*- VM Sprawl - • # of Vm machines exceed network capacity.

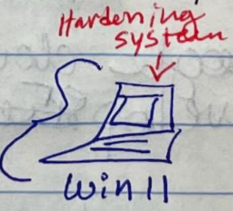
YTB - VM Sprawl ~~and~~. vm Escape

Always Keep vm updated.

Zero Day (0- day) unknown hardware/software flaw that can be exploited.

N-day - Known vulnerability + there IS a patch available.
- flaw is Known to developer
- discovered by hacker or third-party.

Sand boxing - isolation.



Airgap
No internet
No USB
white list
Black-list

misconfiguration
Cryptographic issue -
Key Length

rooting - android devices
jailbreaking = iOS devices (iphone/ipad)

Application Vulnerabilities.
application attack - targets vulnerabilities in OS/apps or architecture/design.

Willian Prado
07/24/2025
Apps & cloud
vulnerabilities

* splicing
* BICSI cert.

Privilege Escalation - get priviledges
vertical
horizontal

Improper Error handling - file not found, fail open errors
|| input ||
"sanitization"

Pointer Deference used to refer to a memory location & not a value.

race condition - multiples threads read & write the same variable. race condition ≅ timing issue!

TechTarget YTB → What is a Race condition (computer programming)

YTB Understand Race conditions: Cause, exploits, & prevention w/ code examples.

Training Course - AWS google cloud Fundamentals
- AWS develop~~[illegible]~~training

Memory injection • attacker introduces (inject) malicious code into a running application's process memory.

YTB - What is memory Leak? attacker introduces (inject) malicious code into a running application's process memory.

Prof. Messer YTB - Memory injection - add code into the memory of an existing process.