Gotta Escape 'Em All

BSides Dublin 2025

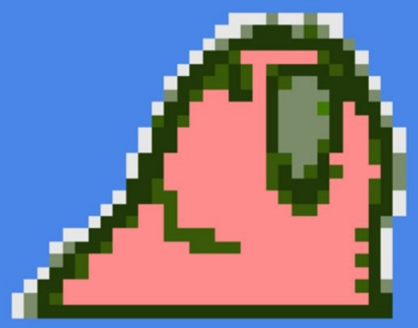
About me

- Senior Security Engineer at Everquote
- Sometimes I can code good!
- Not very sociable so I don't have social media apart from LinkedIn
- I like parrots

Emulators....

So why would you want to hack an emulator?

- Always been interested in video game glitches, especially those used in the speedrunning community for arbitrary code execution
- Got into emulator dev over lockdown... I'll finish it one day...?
- Generally easier to hack someone by phishing or making them download malware



So why would you want to hack an emulator?

- This is incredibly niche and I wouldn't recommend it
- Highly doubt that people are running any console emulators on their work machines
- I just wanted to see what would happen

So, who's broken an emulator before?

- TheZZAZGlitch - old versions of VBA allowed the user to run arbitrary Lua code
- Project64 - had a vuln that allowed arbitary execution
- ZSNES - had a bug where the ROMs could escape the emulator
- Important to note that all of these examples are running on extremely old versions of those emulators

Are you ready for a demostration?

What did we learn?

- Emulators - not the most practical attack vector, but certainty the most fun to break!
- Keep your software updated
- If you're an emulator dev - give a think about security
- And don't download potentially dodgy ROMs ;)

Thanks to!

- The SecEng and SecOps team at Everquote
- (Grant: *he knows what he did*)
- And you, for coming to my talk! You're the best :)