Fiche SEDE

Série de bugs → Exploitation → Vulnérabilité

CVE = Common Vulnerabilities Exposures = Dico des plus grandes vulnérabilité

.0day = première fois découverte exploit

.IE5 onPaintOverflow

Epilogue (integrity data)
↑ Prologue (check data)

Ne pas release le Vendredi

Buffer Overflow ← Stack canari permet de détecter des malloc (integrity de data and data)

~~stack~~

~~sprintf~~ en byte
~~strcpy~~, ~~strcat~~ = truncature détecté, nullterminated, not filled, byte

~~sprintf~~
~~strcpy~~, ~~strcat~~

⚠ Jamais passer taille user contre taille de buffer

malloc n<0 → int overflow
buffer overflow → Préfère écrire son propre Wrapper autour

↳ emalloc wrapper sur malloc check problèmes overflow

Injection ~~over~~ SQL ← Prepare statement } fix SQL injection
← or 1==1;

Negative matching 👎
Positive matching 👍

Format String Attack:

%n peut modifier la variable en param

```
char* c = ~;
printf("coucou %n pd", c);
c → "coucou pd"
```

System(3) } Ouvre des hidden shell
popen(3) }

- "--" stop l'évaluation
- quote les paramètres

↳ wrapper sur 'sh -c xx'

mktemp(3) utilisez peut overide des fichiers sur /tmp

↳ mkstemp ⇒ Fait des checks

- Ne pas utiliser de donnée commun
- d'opérations non-atomiques
- d'opérations avec une mauvaise sémantiques PoF

stat chmod chown

↓ ↓ ↓ file descriptor

fstat fchmod fchown

Faire attention aux :
- Memory handling
- Flow d'exec, control flow
- Hidden state
- User notes
- SIGPIPE
- errno → errno.h
- locales

→ Compiler avec warning
→ Log, beaucoup de log
→ Tracing framework
→ fuzzing tool
↳ injection de données random

Thread → Locker les collections

~~wait~~ → waitpid

autoconf / automake 10 lines changed → 20 000 lines changed

openssl = include fcntl.h

⚠ Différent comportement :
- char (Null terminated vs not null terminated)
- encoding (utf-8, ascii...)
- empty string vs NULL
-

Démarrer programme en root puis switch sur des users moins privilégiés

mac compter → less rights pour l'user

XSS = Cross Site Scripting

Insère du javascript dans un article, injection de données pour faire des bails

↳ sanitize part, with positive matching