

Fiche SEDE

Série de bugs → Exploitation → Vulnérabilité

CVE = Common Vulnerability Exposures = Dico des plus grandes vulnérabilités

0day = première fois découverte exploit

IE5 unoverflow

Epilogue (insert data)

Ne pas release le Vendredi

Buffer Overflow → Stack canari permet de détecter des malifs (insertion de données dans la stack)

strcpy, strcat = truncation detected, null terminated, not filled, byte

! Jamais passer des données dans le buffer

malloc n < 0 → int overflow
buffer overflow

→ Préférer écrire son propre wrapper au pire

↳ emalloc wrapper sur malloc check problèmes overflow

Injection SQL → Prepared statement
or 1==1;

} fix SQL injection

Negative matching
Positive matching

Format String Attack:

%n peut modifier la variable en param

```
char* c = ~;  
printf("coucou %m pd", c);  
c → "coucou pd 7"
```

system(3)
popen(3) } Ouvre des handles shell

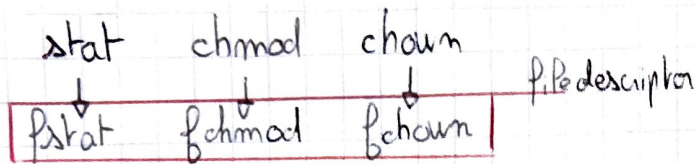
- "--" stop l'évaluation
- quote les paramètres

↳ wrapper sur sh -c x'

mktemp(3) utilises peut override des fichiers sur /tmp

↳ mkstemp → Fait des checks

- Ne pas utiliser de données communes
- d'opérations non-atomiques
- d'opérations avec une mauvaise sémantique



Faire attention aux :

- Memory handling
- Flow d'exec, control flow
- Hidden state
- User notes
- SIGPIPE
- errno → errno.h
- locales
- Thread → Locks, pes collections

Compilers avec warning
Log, beaucoup log
Indexing framework
Fuzzing tool
↳ injection de données rnd

~~wait~~ → waitpid

autoconf / automake 10 lines changed → 20 000 lines changed
openssl = include fcntl.h

⚠ Différents composants :

- 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 complex → peu rights pour l'user

XSS = Cross Site Scripting

Insère du javascripts un article, injection de données pour faire des bails
↳ sanitize path, with positive matching