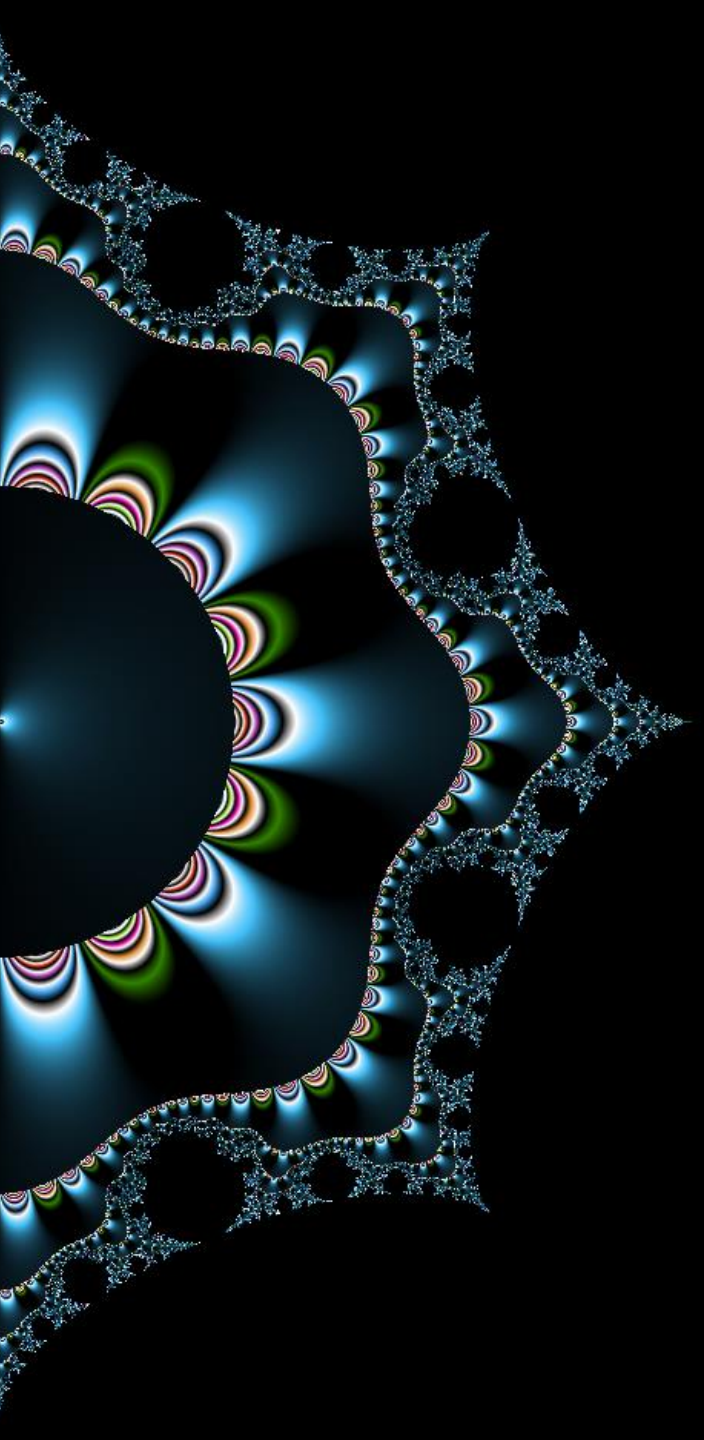

Les vulnérabilités

Et les exploits.

Thibaut HENIN

tbowan@arsouyes.org

C’est quoi une vulnérabilité ?

C’est vrai quoi, il suffirait d’être rigoureux !?

Politique de sécurité

Des bien

(e.g. un serveur)

Des besoin de sécurité

(e.g. confidentialité)

Vulnérabilité

Contournement de la PSSI

Exploit

Programme qui automatise la vulnérabilité

Comment naissent les vulnérabilités ?

C’est vrai quoi, il suffit de faire attention !?

Par Négligence

« Tant que ça marche, on ne touche à rien »

Par conservatisme

« On a toujours fait comme ça ! »

Par dette technique

« C’est trop long de faire propre »

« On corrigera plus tard »

Par Incompétence

« Je ne savais pas »

Par Paresse

« C’est trop chiant »

L’erreur est humaine

« Mince, je ne l’avais pas vu »

Publication !?

Diffuser ou garder pour soi ?

Publier ou pas ?

Troll des années 90

Full disclosure

(publier)

No Disclosure

(garder pour soi)

Forcer la correction

(et devenir célèbre)

Éviter l’exploitation

(et devenir riche)

Responsible Disclosure

Le meilleur des deux mondes

Avertir l’éditeur

(négocier un délais)

Ne publier qu’ensuite

(et devenir célèbre)

Et toucher une récompense

(et devenir riche)

Registre des vulnérabilités

CVE

(Common Vulnerability and Exposure)

Identifiant unique

(CVE-AAAA-NNNN)

Edité par le MITRE :

https://www.mitre.org/ & https://cve.mitre.org/

Mesure du Risque (score cvss)

Score de base

Options

Vraisemblance

Exploitation

Vecteur, Complexité, Authentification

Temporelle

Exploit, correctif, confiance

Gravité

Impact

Confidentialité, Intégrité, Disponibilité

Environnement

Contexte d’utilisation

Quelle attitude ?

Pourquoi y jouer ?

Dissymétrie de l’affrontement

	Gentils	Méchants
Défaite	Conséquences Globalement graves	-
Victoire	-	Conséquences Globalement positives

Autruche optimiste

Ça marche, tout va bien

On verra plus tard

Qui voudrait nous attaquer ?

Perfectionniste paranoïaque

Tout doit être parfait

Une vulnérabilité est preuve d’incompétence

Il reste toujours un risque

Humilité constructive

Où sont les faiblesses

Comment les corriger

Amélioration continue

« Ce n’est pas parfait, mais on y travaille »