DogCat

Axel Thouvenin & Juliette Bluem

27 septembre 2021

Table des matières

Partie I : Contrôle

Partie II : Contexte

Partie III : Résumé

niveau de risque global : assez grave

Partie IV : Vulnérabilités

1 LFI

1.1 risques

8.1 (élevé) + 6.25 (elevee) => elevee

1.2 description

Un utlisateur peut pénétrer sur le serveur de DogCat et ainsi insérer un fichier de son choix. Cela peut engendrer de la fuite d'informations.

1.3 hotes/url impactés

$http://ip/?view=dog$

1.4 rémédiation

Remplacer le "contains" par un "=" afin de n'accepter que les fichier dog.php et cat.php.
Filtrer les entrées utilisateurs(pa ;ramètre dans l'url). Dans le cas présent que les fichiers dog.php et cat.php.

1.5 details de l'exploitation

Dans le cas présent "$view=dogs$" nous a permit de voir qu'un ajout est effectué.

2 Accès en lecture/ecriture des access.log

2.1 risques

9.1 crtique / 6.75 elevé => CRITIQUE

2.2 description

Accédé via la LFI. log poisoning

2.3 hotes/url impactés

$http://ip/?view=dog$

2.4 rémédiation

Empêcher la lecture des logs par l'utilisateur www-data.

2.5 details de l'exploitation

3 Mauvaise configuration de sudo

3.1 risques

7.8 (eleve) / 5.75 (medium) => moyen

3.2 description

Mauvaise config de sudo pouvant entrainer une elevation de privilèges

3.3 hotes/url impactés

@ip

3.4 rémédiation

www.data n'est pas un user classique, il ne doit etre utilisé uniquement par le server web et ne doit pas avoir de droits sudo

3.5 details de l'exploitation

4 Mauvaise configuration de la sauvegarde

4.1 risques

8.2 eleee / 5 moyen => moyen

4.2 description

sauvegarde executé depuis le serveur mais scripte hebergé sur le docker. On peut donc partir du docker

4.3 hotes/url impactés

@ip

4.4 rémédiation

ne pas heberger le scrypte de sauvegarde sur le docker

4.5 details de l'exploitation

partie backups

Partie V : Plan d'actions

1243 ou 2143 selon contexte