



DogCat

Axel Thouvenin & Juliette Bluem

27 septembre 2021



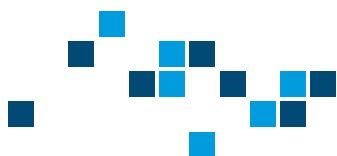
**UNIVERSITÉ
DE LORRAINE**

LORRAINE INP
les talents se lèvent à l'Est



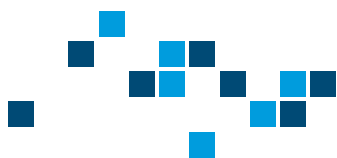
Table des matières

I	Contrôle	3
II	Contexte	4
III	Résumé	5
IV	Vulnérabilités	6
1	LFI	6
1.1	risques	6
1.2	description	6
1.3	hotes/url impactés	6
1.4	remédiation	6
1.5	details de l'exploitation	6
2	Accès en lecture/écriture des access.log	6
2.1	risques	6
2.2	description	6
2.3	hotes/url impactés	6
2.4	remédiation	6
2.5	details de l'exploitation	6
3	Mauvaise configuration de sudo	7
3.1	risques	7
3.2	description	7
3.3	hotes/url impactés	7
3.4	remédiation	7
3.5	details de l'exploitation	7
4	Mauvaise configuration de la sauvegarde	7



4.1	risques	7
4.2	description	7
4.3	hotes/url impactés	7
4.4	rémédiation	7
4.5	détails de l'exploitation	7

V	Plan d'actions	8
---	----------------	---



Partie I : Contrôle

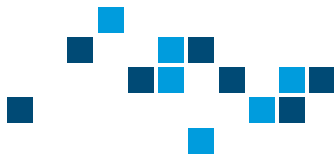


Partie II : Contexte



Partie III : Résumé

niveau de risque global : assez grave



Partie IV : Vulnérabilités

1 LFI

1.1 risques

8.1 (élevé) + 6.25 (elevation) => élevée

1.2 description

Un utilisateur 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 notes/url impactés

http : //ip/?view = dog

1.4 remédiation

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

1.5 détails de l'exploitation

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

2 Accès en lecture/écriture des access.log

2.1 risques

9.1 critique / 6.75 élevé => CRITIQUE

2.2 description

Accédé via la LFI. log poisoning

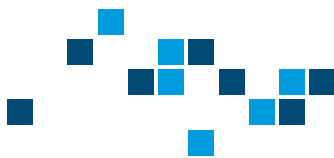
2.3 notes/url impactés

http : //ip/?view = dog

2.4 remédiation

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

2.5 détails de l'exploitation



3 Mauvaise configuration de sudo

3.1 risques

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

3.2 description

Mauvaise config de sudo pouvant entraîner une élévation de privilèges

3.3 hotes/url impactés

@ip

3.4 remédiation

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

3.5 détails de l'exploitation

4 Mauvaise configuration de la sauvegarde

4.1 risques

8.2 eleee / 5 moyen => moyen

4.2 description

sauvegarde exécuté depuis le serveur mais scripte hébergé sur le docker. On peut donc partir du docker

4.3 hotes/url impactés

@ip

4.4 remédiation

ne pas héberger le scripte de sauvegarde sur le docker

4.5 détails de l'exploitation

partie backups



Partie V : Plan d'actions

1243 ou 2143 selon contexte