PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification
ANSSI-CSPN-2024/02

Nftables (sous-système du noyau Linux)

Version Debian 12.1 / Noyau Linux 6.1.55-1

Paris, le 14 Juin 2024

Le Directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2024/02**
Nom du produit **Nftables (sous-système du noyau Linux)**
Référence/version du produit **Version Debian 12.1 / Noyau Linux 6.1.55-1**
Catégorie de produit **Pare-feu**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **ANSSI** 51 boulevard de la Tour-Maubourg 75700 Paris, France
Développeur **THE NETFILTER.ORG PROJECT** https://netfilter.org
Centre d'évaluation **SYNACKTIV** 5 boulevard Montmartre 75002 Paris, France
Fonctions de sécurité évaluées Application des règles de filtrage Fiabilité du noyau de filtrage Fiabilité de l'interface d'administration Journalisation
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Nftables (sous-système du noyau Linux), Version Debian 12.1 / Noyau Linux 6.1.55-1 » développé par THE NETFILTER.ORG PROJECT.

Ce produit est un sous-système du noyau Linux qui permet le filtrage et la classification des paquets réseaux.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☒	**3**	**pare-feu**
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	Nftables (sous-système du noyau Linux)
Numéro de la version évaluée	Version Debian 12.1 / Noyau Linux 6.1.55-1

La version certifiée du produit peut être identifiée à partir d'un *shell* en utilisant la commande « *uname -a* » et « *cat /etc/debian_version* » :

```
user@debian:~$ uname -a
Linux debian 6.1.55+ #1 SMP PREEMPT_DYNAMIC Tue Oct 3 10:28:04 CEST 2023 x86_64 GNU/Linux

user@debian:~$ cat /etc/debian_version
12.1
```

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

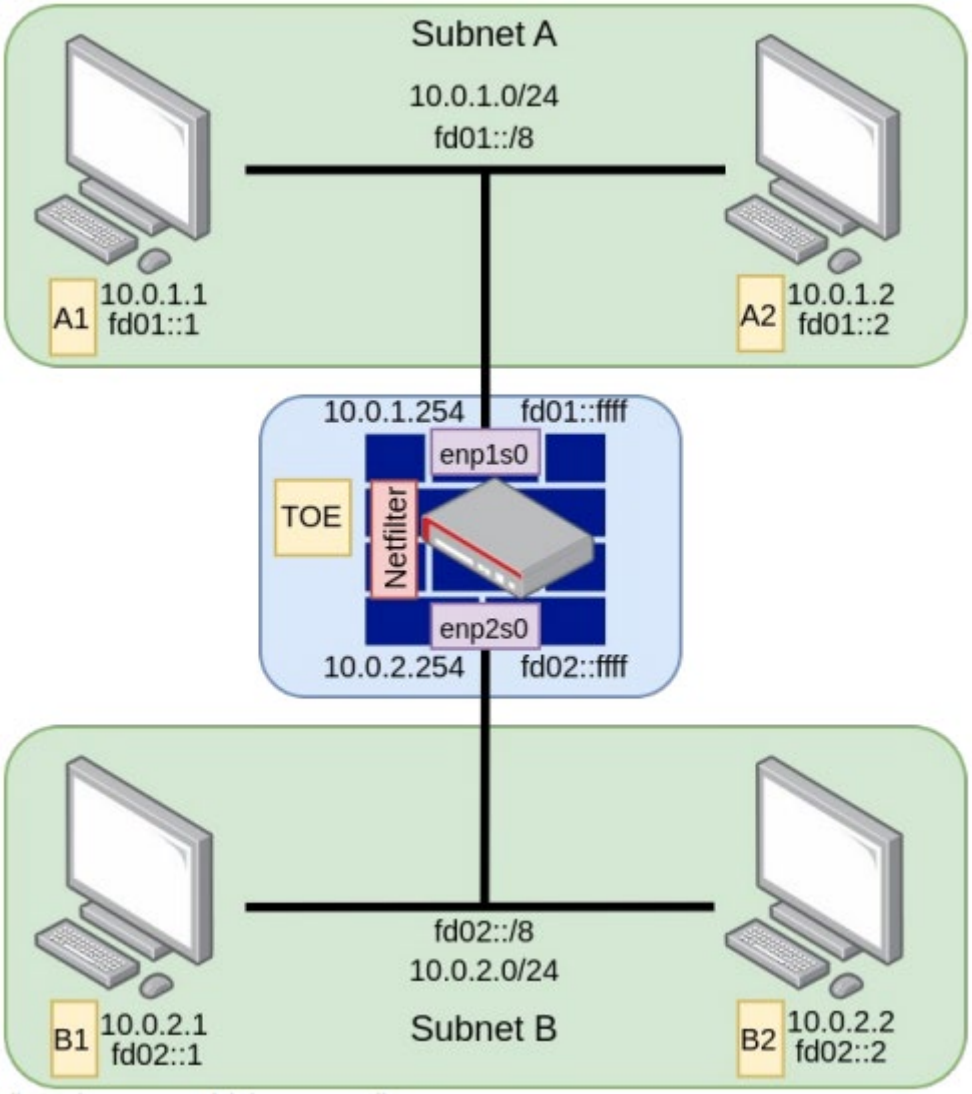
- Application des règles de filtrage ;
- Fiabilité du noyau de filtrage ;
- Fiabilité de l'interface d'administration ;
- Journalisation.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à une installation par défaut d'une distribution Debian.

La plateforme de test est constituée des éléments suivants :

- Des machines virtuelles ;
- L'infrastructure de test comprend un certain nombre de sous-réseaux.



2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'installation du noyau Linux incluant le produit comporte les étapes suivantes :

- Installation de la distribution Debian avec l'utilitaire « nftables » ;
- téléchargement du code source du noyau Linux appartenant à la distribution Debian ;
- application du patch pour se prémunir de la CVE-2023-5197 ;
- compilation du noyau Linux avec la configuration par défaut ;
- installation du noyau Linux compilé.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source*

L'évaluateur a revu le code source des composants « defrag » et « conntrack » du produit évalué.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

La distribution Debian doit être configurée de telle sorte qu'un utilisateur non privilégié ne puisse faire usage du « *user namespace* ».

Les risques identifiés lors de l'évaluation entraînent des recommandations d'usage pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier à des environnements UNIX.

2.2.7.3 Notes et remarques diverses

Une remarque concernant le manque de confiance du code source de l'interface d'administration : deux vulnérabilités 0 jour ont été remontées depuis la fin de l'audit sur cette surface.

2.3 Analyse de la résistance des mécanismes cryptographiques

Le produit ne comporte pas de mécanismes cryptographiques.

2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'évaluation.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Nftables (sous-système du noyau Linux), Version Debian 12.1 / Noyau Linux 6.1.55-1 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], suivre les recommandations se trouvant dans les guides fournis [GUIDES], et de plus :

- Mettre la variable *« kernel.unprivileged_userns_clone »* à « 0 ».

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - *CSPN security target - nftables,* référence CSPN_TARGET_NFTABLES_1.3, version 1.3, 25 avril 2024.
[RTE]	Rapport technique d'évaluation : - RTE CSPN nftables, référence CSPN-2023-NFTABLES, version 1.2, 25 avril 2024.
[GUIDES]	Guide d'utilisation du produit : - https://wiki.nftables.org/wiki-nftables/index.php/Main_Page

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.