RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Secretariat-General for Defence
and National Security

French National Cyber
Security Agency

Certification report
ANSSI-CSPN-2024/02

Nftables (Linux kernel subsystem)

Debian 12.1 / Linux kernel 6.1.55-1 Release

Courtesy translation

Paris, 14 June 2024

The Deputy Director General of the Agence nationale de la sécurité des systèmes d'information (French National Cyber Security Agency)

Emmanuel NAEGELEN

[ORIGINAL SIGNATURE]

SÉCURITÉ CERTIFICATION

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

WARNING

This report is intended to provide sponsors with a document enabling them to certify the level of security offered by the product under the conditions of use or operation defined in this report for the version that has been evaluated. It is also intended to provide the potential purchaser of the product with the conditions under which the purchaser will be able to operate or use the product in such a way as to achieve the conditions of use for which the product has been evaluated and certified.This is why the user must read the certification report along with the assessed user and administration guides and the product's security target, which describes the threats, the assumptions about the environment and the presupposed conditions of use, so users can assess whether the product meets their needs in terms of security objectives.

Certification does not in itself constitute a recommendation of the product by the French National Cyber Security Agency (ANSSI) and does not guarantee that the certified product is totally free of exploitable vulnerabilities.

Any correspondence relating to this report should be addressed to :

Secretariat-General for Defence and National Security
French National Cyber Security Agency
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Certification report reference **ANSSI-CSPN-2024/02**
Product name **Nftables (Linux kernel subsystem)**
Product reference/version **Debian 12.1 / Linux kernel 6.1.55-1 Release**
Product category **Firewall**
Evaluation criteria and version **FIRST-LEVEL SECURITY CERTIFICATION** **(CSPN)**
Sponsor **ANSSI** 51 boulevard de la Tour-Maubourg 75700 Paris, France
Developer **THE NETFILTER.ORG PROJECT** https://netfilter.org
Assessment centre **SYNACKTIV** 5 boulevard Montmartre 75002 Paris, France
Security functions assessed Application of filtering rules Reliability of the filter core Reliable administration interface Logging
Security functions not evaluated Not applicable
Restriction(s) on use Yes (see §3.2)

PREFACE

Certification

Certification of the security offered by information technology products and systems is governed by Decree 2002-535 of 18 April 2002, as amended. This decree states that :

- the Agence nationale de la sécurité des systèmes d'information (French National Cyber Security Agency) prepares the certification reports. These reports specify the characteristics of the proposed security objectives. They may include any warning that the editors deem appropriate to mention for security reasons. They may or may not be disclosed to third parties or made public, at the discretion of the sponsor (article 7);
- the certificates issued by the Director General of the French National Cyber Security Agency attest that the copy of the products or systems submitted for evaluation meets the specified security characteristics. They also certify that the assessments have been carried out in accordance with the rules and standards in force, with the required competence and impartiality (article 8).

CSPN certification procedures are available on the following website cyber.gouv.fr.

TABLE OF CONTENTS

1 The product

1.1 Product presentation

The product under evaluation is "Nftables (Linux kernel subsystem), Debian Release 12.1 / Linux Kernel 6.1.55-1" developed by THE NETFILTER.ORG PROJECT.

The product is a subsystem of the Linux kernel that filters and classifies network packets.

1.2 Description of the product evaluated

The security target [ST] defines the evaluated product, its evaluated security features and its operating environment.

1.2.1 *Product category*

£ 1	intrusion detection
£ 2	anti-virus, protection against malicious code
T **3**	**firewall**
£ 4	data erasure
£ 5	security administration and supervision
£ 6	identification, authentication and access control
£ 7	secured communication
£ 8	secure messaging
£ 9	secure storage
£ 10	secure run-time environment
£ 11	Set top box (STB)
£ 12	embedded hardware and software
£ 13	programmable logic controller
£ 99	other

1.2.2 Product *identification*

Product	
Product name	Nftables (Linux kernel subsystem)
Number of the evaluated version	Debian 12.1 / Linux kernel 6.1.55-1 Release

The certified version of the product can be identified from a *shell* with the command " *uname -a* " and " *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 *Security functions*

The security functions assessed for the product are :

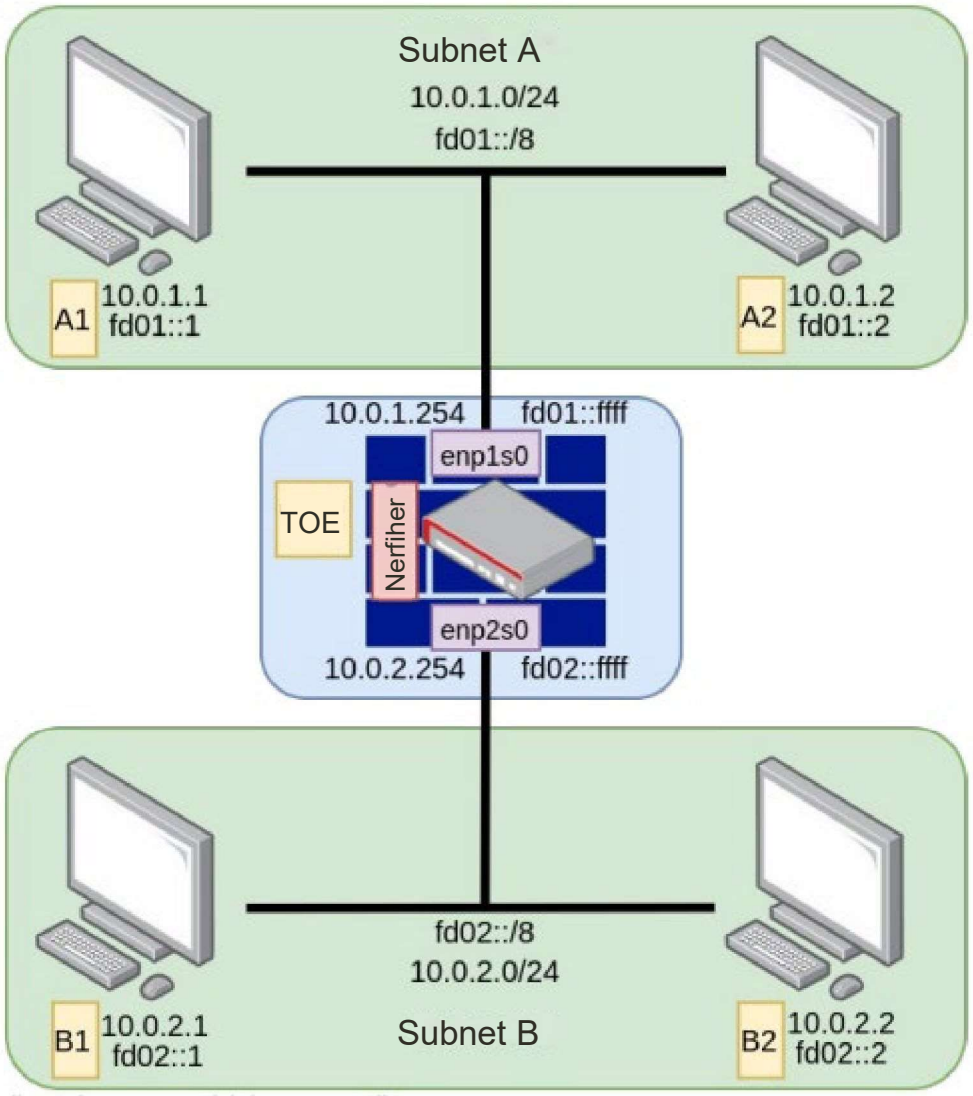
- Application of filtering rules;
- Reliability of the filter core;
- Reliability of the administration interface;
- Logging.

1.2.4 *Configuration evaluated*

The configuration evaluated corresponds to a default installation of a Debian distribution.

The test platform consists of the following elements:

- Virtual machines;
- The test infrastructure includes a number of sub-networks.



2 Evaluation

2.1 Evaluation standards

The evaluation was carried out in accordance with the First Level Security Certification [CSPN].

2.2 Evaluation work

The evaluation work was performed on the basis of the security requirements, sensitive assets, threats, users and security functions defined in the security target [ST].

2.2.1 *Installing the product*

2.2.1.1 Environment setting details and installation options

The product was evaluated in the configuration specified in paragraph 1.2.4.

2.2.1.2 Description of the installation and any non-conformities

Installation of the Linux kernel including the product involves the following steps:

- Install the Debian distribution with the "nftables" utility;
- download the source code of the Linux kernel belonging to the Debian distribution;
- apply the patch to protect against CVE-2023-5197;
- compilation of the Linux kernel with the default configuration;
- installation of the compiled Linux kernel.

2.2.1.3 Miscellaneous notes and remarks

Not applicable.

2.2.2 *Analysis of documentation*

The evaluator had access to the documents [GUIDES] as part of this evaluation.

The product guides enable the product to be installed and used without causing accidental safety hazards.

2.2.3 *Source code review*

The evaluator has reviewed the source code of the "defrag" and "conntrack" components of the product under evaluation.

This analysis contributed to the compliance and resistance analysis of the product's security functions.

2.2.4 *Analysis of security function compliance*

All the security functions tested were found to comply with the security target [CDS].

2.2.5 *Analysis of the resistance of security function mechanisms*

All the security functions have undergone penetration testing, and none of them has a vulnerability that could be exploited in the context in which the product is used and by the level of attacker targeted.

2.2.6 *Vulnerability analysis (design, construction, etc.)*

2.2.6.1 List of known vulnerabilities

No known exploitable vulnerabilities affecting the evaluated version of the product have been identified.

2.2.6.2 List of vulnerabilities discovered during the evaluation and expert opinion

No vulnerability specific to the product or its implementation has been discovered that could question the security of the product.

2.2.7 *Analysis of ease of use*

2.2.7.1 Cases where security is called into question

The Debian distribution must be configured in such a way that an unprivileged user cannot use the *user namespace*.

The risks identified during the evaluation lead to recommendations for use by the user (see chapter 3.2).

2.2.7.2 Expert opinion on ease of use

Overall, the product is well documented, and implementation is straightforward for users familiar with UNIX environments.

2.2.7.3 Miscellaneous notes and remarks

A comment about the lack of confidence in the administration interface source code: two 0-day vulnerabilities have been reported since the end of the audit on this surface.

2.3 Analysis of the resistance of cryptographic mechanisms

The product does not include cryptographic mechanisms.

2.4 Analysis of the hazard generator

The product does not include a hazard generator within the scope of the evaluation.

3 Certification

3.1 Conclusion

The evaluation was carried out in accordance with the rules and standards in force, with the competence and impartiality required of an approved evaluation centre.

This certificate attests that the product "Nftables (Linux kernel subsystem), Debian Release 12.1 / Linux Kernel 6.1.55-1" submitted for evaluation meets the security characteristics specified in its security target [ST] for the level of evaluation expected at the time of a first-level security certification.

3.2 Recommendations and restrictions on use

This certificate relates to the product specified in chapter 1.2 of this certification report.

The user of the certified product must ensure compliance with the environmental security objectives specified in the security target [CDS], follow the recommendations in the guides provided [GUIDES], and in addition:

- Set the *"kernel.unprivileged_userns_clone"* variable to "0".

ANNEX A. Documentary references for the product evaluated

[CDS]	Reference security target for evaluation: - *CSPN security target - nftables,* reference CSPN_TARGET_NFTABLES_1.3, version 1.3, 25 April 2024.
[RTE]	Technical evaluation report: - RTE CSPN nftables, reference CSPN-2023-NFTABLES, version 1.2, 25 April 2024.
[GUIDES]	Product User Guide: - https://wiki.nftables.org/wiki-nftables/index.php/Main_Page

ANNEX B. Certification references

Decree 2002-535 of 18 April 2002, as amended, on the evaluation and certification of the security offered by information technology products and systems.	
[CSPN]	First-level security certification of information technology products, reference ANSSI-CSPN-CER-P-01, version 5.0, 12 January 2023. Criteria for assessment with a view to first-level security certification, reference ANSSI-CSPN-CER-P-02, version 4.0, 28 March 2020. Methodology for assessment with a view to first-level security certification, reference ANSSI-CSPN-NOTE-01, version 3.0,6 September 2018.