Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2013/07

rWeb
Version 4.1 Feature Pack 1

Paris, le 27 juin 2013

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2013/07**
Nom du produit **rWeb**
Référence/version du produit **4.1 Feature Pack 1**
Catégorie de produit **Pare-feu**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Deny All** **63 ter, avenue Edouard Vaillant** **92100 Boulogne-Billancourt** **France**
Commanditaire **Deny All** **63 ter, avenue Edouard Vaillant** **92100 Boulogne-Billancourt** **France**
Centre d'évaluation **SOGETI** **24, rue du gouverneur Eboué** **92130 Issy les Moulineaux**

Préface

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 Premier ministre 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 sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « rWeb**,** version 4.1 Feature Pack 1 **»** développé par la société Deny All.

rWeb est un pare-feu applicatif. Il analyse les requêtes à destination d'un serveur web afin de bloquer les tentatives d'attaques.

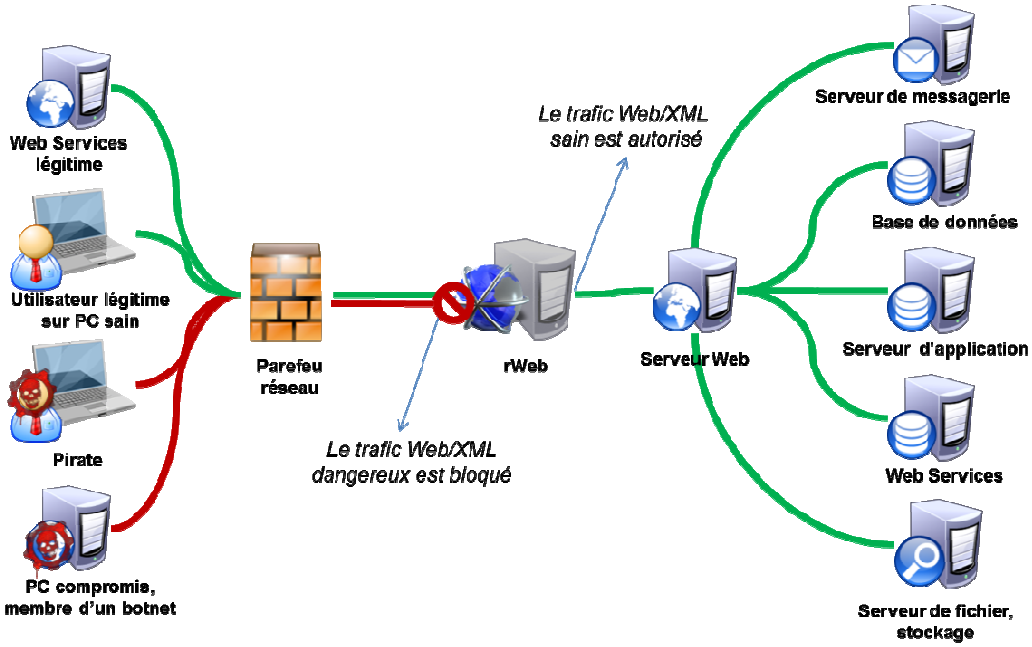


Figure 1

rWeb est basé sur une technologie de *reverse proxy* et filtre la totalité des flux applicatifs HTTP/HTTPS, SOAP et XML.

rWeb est disponible en version logicielle, installable sous Linux, mais aussi sous la forme d'une image VMware ou encore en « *bundle* » avec une *appliance* standard HP.

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 – firewall**
☐ 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 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

La version certifiée du produit, « 4.1 FP1 », est identifiable via l'interface d'administration.

Pour connaitre la révision exacte du produit, il est nécessaire de se connecter localement sur le produit et de regarder le fichier /opt/rweb/share/rweb/patches.

Le package **daos10-1.2-0_x86_64.iso** utilisé pour la présente évaluation a l'empreinte SHA-1 suivante :

6bafdf2e15051079be63aae275b0fc10d6158778

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la mise en œuvre de la politique de sécurité, comprenant :
  - l'analyse de la conformité protocolaire ;
  - la détection d'attaques ;
  - le filtrage des messages d'erreurs émis par les serveurs web ;
- le blocage des attaques suite à leur détection ;
- la journalisation des évènements et des actions.

1.2.4. Configuration évaluée

La politique de filtrage utilisée dans la configuration évaluée est la politique « *Maximum Security Policy* » activant notamment l'ensemble des options et modules de sécurité.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 25 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 « Description du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 5 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

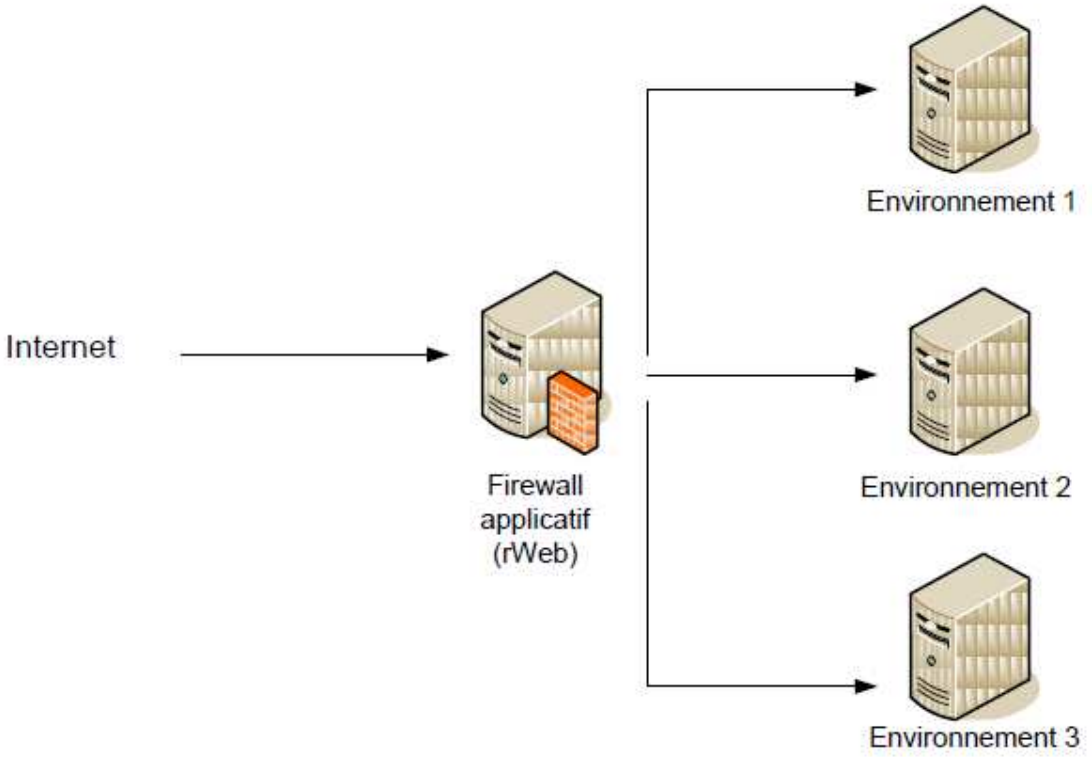
Conforme à la cible de sécurité [CDS] (chapitre 2.7 « Description des utilisateurs typiques »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

L'architecture nécessaire à la réalisation de l'évaluation a été déployée à l'aide de machines virtuelles, dans un souci de reproductibilité des tests et de stockage des archives. Pour ce faire, le logiciel **VMware Workstation** a été utilisé dans sa version **8.0.0 build 471780**.

L'architecture mise en place est résumée sur le schéma suivant :



rWeb a été installé sur DaOS 10, une distribution Linux reposant sur CentOS 6.4, à partir du package **daos10-1.2-0_x86_64** téléchargé sur le site de Deny All.

Sur la plate-forme de test déployée, rWeb protège 3 serveurs virtuels :

- **Environnement 1 :** machine virtuelle utilisant le système d'exploitation Linux Debian 5.0.7, sur laquelle le serveur Web Apache 2.2.9 et le serveur MySQL 5.0.51a fournissent l'application PHP « drupal », à protéger ;
- **Environnement 2 :** machine virtuelle utilisant le système d'exploitation Windows Server 2003, sur laquelle le serveur Web IIS 6.0 et le serveur SQL Server Express 2005 fournissent l'application ASP.NET « DotNetNuke », à protéger ;
- **Environnement 3 :** machine virtuelle utilisant le système d'exploitation Linux Debian 5.0.3, sur laquelle le serveur applicatif Apache Tomcat et le serveur SQL HSQLDB fournissent l'application J2EE « uPortal », à protéger.

2.3.2.2. Particularités de paramétrage de l'environnement

Sans objet.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

Lors de l'installation, l'utilisateur est amené à définir 3 mots de passe pour le compte administrateur, le compte utilisateur et le compte *superadmin* gérant l'interface d'administration. Bien que des restrictions soient imposées pour la complexité du mot de passe des comptes administrateur et superadmin, cela n'est pas le cas pour le compte utilisateur.

Lors de l'installation avec un disque virtuel de 20 Go, une erreur de partitionnement empêche de continuer l'installation. Le problème est résolu en augmentant la taille du disque virtuel.

2.3.2.5. Durée de l'installation

Sans objet.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDE]. La documentation est claire et aucune non-conformité majeure n'a été relevée.

La politique de sécurité « *Maximum Security Policy* » n'est pas mentionnée explicitement dans la documentation.

2.3.4. Revue du code source (facultative)

Les évaluateurs n'ont pas eu accès au code source.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Analyse de la conformité protocolaire	**Réussite**
Détection des attaques	**Réussite**
Action préventives	**Réussite**
Blocage des attaques	**Réussite**
Journalisation des évènements	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Sans objet.

2.3.8. Avis d'expert sur le produit

Dans la configuration « *Maximum Security Policy* », rWeb 4.1 détecte, bloque et journalise correctement les attaques courantes.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Liste noire
Blocage des injections SQL
Blocage des *directory traversal*
Blocage des injections de commandes
Détection des XSS
Filtrage des réponses
Réduction des chemins d'accès en forme canonique

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Comme tout système de filtrage, rWeb a des limites. Ainsi, il sera toujours possible de contourner le filtrage en cherchant des variations ou des encodages non gérés par rWeb. Cependant, l'ensemble des fonctionnalités et des modules de la version évaluée apporte un bon niveau de protection en détectant de manière assez générique les principaux types d'attaques.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

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

Aucune.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Comme indiqué dans le §1.2.3 du présent rapport, la configuration évaluée est la politique de sécurité « *Maximum Security Policy* », il est donc important de configurer le produit avec cette politique.

Les comptes administrateur, utilisateur et *superadmin* doivent être protégés par un mot de passe robuste[1].

Les administrateurs du produit doivent avoir une bonne connaissance du protocole http, des attaques Web et des expressions régulières pour utiliser et configurer efficacement le produit.

[1] Des recommandations de sécurité relatives aux choix des mots de passe sont disponibles sur le site de l'ANSSI www.ssi.gouv.fr.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

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 « rWeb**,** version 4.1 Feature Pack 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. 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 d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité rWeb4 ;* Version : *1.2* ; Date : *19/02/2013*.
[RTE]	*Evaluation CSPN de rWeb 4.1 FP1 ;* Référence : *U12.ESEC.CR2013.022* ; Date : *15/05/2013*.
[GUIDE]	*Protect 4.1 FP1 – User Guide ;* Version : *1.0* ; Date : *08/04/2013*.

Annexe 2. Références 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 (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr.
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr.