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-2013/11

Wallix AdminBastion
Version 3.1.9 avec correctifs de sécurité 3354, 5420 et 5435

Paris, le 25 novembre 2013

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

[ORIGINAL SIGNE]
Patrick PAILLOUX

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-2013/11**
Nom du produit **Wallix AdminBastion**
Référence/version du produit **Version 3.1.9 avec correctifs de sécurité 3354, 5420 et 5435**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Wallix** **118 rue de Tocqueville** **75017 Paris** **France**
Commanditaire **Wallix** **118 rue de Tocqueville** **75017 Paris** **France**
Centre d'évaluation **OPPIDA** **6 avenue du Vieil Etang – Bât. B** **78180 Montigny-le-Bretonneux** **France**

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 « Wallix AdminBastion**,** version 3.1.9 avec correctifs de sécurité 3354, 5420 et 5435 **»** développé par la société Wallix.

Wallix AdminBastion (WAB) est une plateforme offrant des fonctionnalités de relais applicatif (proxy) permettant de contrôler et de tracer les accès à des ressources informatiques (serveurs, équipements réseau, services).

Le produit permet ainsi de contrôler les accès aux ressources sensibles par des prestataires, des comptes à privilèges ou des utilisateurs à risque et d'enregistrer les sessions de travail à des fins d'audit ou d'investigation. Dans ce but, il offre des fonctionnalités d'authentification unique (*Single Sign-On, SSO*), de relais applicatif et de stockage sécurisé des données d'authentification.

WAB est prévu pour fonctionner en *appliance* matérielle. Il est livré installé sur des serveurs *Dell R320* ou *R520* avec carte de supervision à distance *iDrac* et alimentation redondante.

Le WAB peut être déployé selon l'un de ces deux modes de fonctionnement:

1. *Standalone* : le système tourne sur une seule *appliance* ;
2. HA[1]: le système tourne sur deux *appliances* en mode actif-passif. Une liaison doit être établie entre les ports Ethernet 1 de chaque machine (configuration évaluée).

[1] *High Availability* ou Haute disponibilité.

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 est identifiable par les éléments suivants :

- Numéro de version : 3.1.9.

  Ce numéro de version peut être vérifié, via l'interface Web du produit, dans le menu 'Audit système', rubrique 'Etat du système', ou en exécutant le script **`/opt/wab/bin/WABVersion`** sur l'interface d'administration locale.

- Correctifs de sécurité 3354, 5420 et 5435.

  La commande **`dpkg -l | grep wab`** exécutée sur l'interface d'administration locale fait apparaître la liste de paquets suivante, correspondant à la version 3.1.9 à jour des correctifs 3354, 5420 et 5435 :

```
ii backend 3.1.9.13382-wab2-3.1.9.2-wallix1 Wallix Admin Bastion
database backend
ii models 3.1.9.13382-wab2-3.1.9.2-wallix1 WAB python model for ACL used
for wab 3.1 and later
ii wab2 3.1.9.13382-wab2-3.1.9.2-wallix1 Wallix AdminBastion Main meta
package
ii wab2-core 3.1.9.14607-wab2-3.1.9-wallix1 Wallix AdminBastion Core
Package
ii wab2-gui 3.1.9.14607-wab2-3.1.9-wallix1 Wallix AdminBastion Web GUI
ii wab2-ha 3.1.9.13382-wab2-3.1.9.2-wallix1 Wallix AdminBastion HA
management
ii wab2-system-configuration 3.1.9.13382-wab2-3.1.9.2-wallix1 Wallix
System Configuration
ii wabchgpwd 3.1.9.13382-wab2-3.1.9.2-wallix1 Wallix Admin Bastion main
service, provides WAB feature over a single network service.
ii wabconfig 3.1.9.13382-wab2-3.1.9.2-wallix1 wabconfig library.
```

```
ii wabcrypto 3.1.9.14542-wab2-3.1.9-wallix1 WAB module that provides
crypto functionalities.
ii wabengine 3.1.9.14542-wab2-3.1.9-wallix1 Wallix
```

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :

- authentification unique : les utilisateurs des ressources cibles n'ont plus besoin de présenter des secrets d'authentification sur chacune des ressources cibles. Ils s'authentifient auprès du WAB qui, après s'être assuré que les accès sont autorisés, ouvre l'accès à la ressource demandée ;
- changement des mots de passe des ressources cibles (Windows et UNIX), périodiquement ou à la demande ;
- contrôle des accès aux ressources cibles : le WAB permet de mettre en place une politique de contrôle d'accès ;
- traçabilité : placé en coupure entre l'utilisateur et la ressource cible, le WAB permet d'enregistrer toutes les opérations réalisées, et ceci pour tous les protocoles supportés.

1.2.4. Configuration évaluée

Dans le cadre de l'évaluation et comme indiqué dans la cible de sécurité [CDS], le produit a été livré installé sur des serveurs Dell R320.
Deux WAB ont été connectés entre eux en mode HA, dans un sous-réseau privé, et ont été configurés conformément à la documentation (voir [GUIDES]).
Les correctifs de sécurité 3354, 5420 et 5435 ont été livrés séparément, accompagnés d'un guide d'installation, et installés par l'évaluateur. Pour chaque correctif, un script permet la vérification de l'intégrité du code.

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 par la procédure CSPN.

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 « Argumentaire (description) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « 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 2.5 « Utilisateurs typiques du produit »).
Le terme « utilisateurs » désigne les administrateurs des ressources cibles placées derrière le WAB. Le terme « administrateurs » désigne les administrateurs du WAB.

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

La plate-forme de test est constituée de deux WAB connectés entre eux en mode actif-passif (mode HA), dans un sous-réseau privé.
Des machines virtuelles sont utilisées en tant que ressources cibles.
L'accès au WAB pour les tests est réalisé depuis le réseau privé de l'évaluateur, conformément aux hypothèses de la cible.

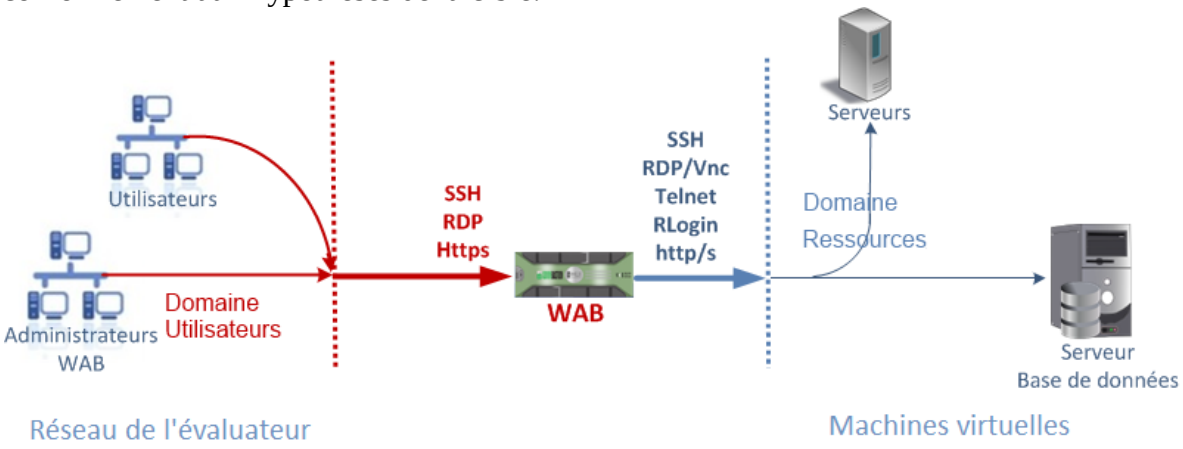

Figure 1 Environnement de test du produit

2.3.2.2. Particularités de paramétrage de l'environnement

Dans la configuration évaluée les deux WAB sont connectés à des domaines ressources et utilisateurs non accessibles depuis internet[1], conformément aux hypothèses sur l'environnement.
De même, les membres du domaine « utilisateurs » ne peuvent pas accéder aux ressources cibles sans passer par le WAB.

2.3.2.3. Options d'installation retenues pour le produit

Dans le cadre de l'évaluation, le mode d'utilisation HA (Haute disponibilité) a été activé.

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

Sans objet.

2.3.2.5. Durée de l'installation

L'installation a nécessité une journée.

2.3.2.6. Notes et remarques diverses

L'installation du produit et sa configuration initiale sont bien documentées et peuvent être réalisées facilement. La configuration du mode HA, bien que moins précisément documentée, n'a pas non plus posé de problème particulier à l'évaluateur.

[1] Certaines machines du domaine ressource peuvent être connectées à Internet, mais les fonctions d'administration ne sont pas accessibles en dehors du réseau privé dans lequel est installé le WAB.

Enfin, la configuration applicative du WAB nécessite une bonne compréhension du fonctionnement du produit pour être correctement réalisée.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et globalement précise. Aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

Les évaluateurs ont eu accès à la partie du code source implémentant le relais applicatif RDP. Le code est clair et l'évaluation n'a pas mis en évidence de manquement manifeste aux bonnes pratiques de programmation.
Pour le reste les évaluateurs n'ont pas eu accès au code source et les tests ont donc été réalisés en boîte noire.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification unique	**Réussite**
Changement des mots de passe sur les ressources cibles	**Réussite**
Contrôle des accès aux ressources cibles	**Réussite**
Traçabilité des opérations réalisées	**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

Le fonctionnement du produit est conforme à ses spécifications fonctionnelles.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Les fonctions listées au 2.3.5 ont été évaluées.

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Le WAB dans sa version évaluée offre des mécanismes globalement robustes et à l'état de l'art.

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

Un utilisateur légitime connecté peut sous certaines conditions réaliser un déni de service sur la console SSH. Ce scénario est jugé hors cible.
Par ailleurs, l'évaluateur a mis en évidence que certaines fonctions étaient théoriquement vulnérables à des attaques dont la mise en œuvre sur la configuration évaluée et dans le cas d'usage considéré nécessite des capacités jugées supérieures à ce qui est attendu dans le cadre d'une CSPN ; ces vulnérabilités sont donc considérées comme résiduelles par l'évaluateur.

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

Sans objet.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Le certificat par défaut du serveur RDP repose sur l'algorithme SHA1, non conforme au RGS. Il doit être changé par l'utilisateur via l'interface SSH du WAB. Ceci est précisé au chapitre 7 du guide de démarrage rapide (voir [GUIDES]).
De même, le certificat par défaut du proxy HTTPS repose sur SHA1 et doit être remplacé conformément aux recommandations contenues dans [GUIDES].

La clé maîtresse du bastion est protégée par un mot de passe. L'administrateur devra s'assurer de choisir un mot de passe respectant les règles et recommandations contenues dans [GUIDE-ANSSI].

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

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste de référence des mécanismes cryptographiques est celle fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY]. La résistance de ces mécanismes a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [RTE] et concluent que, si les recommandations présentes dans [GUIDES] sont appliquées, les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de l'ANSSI (voir [REF-CRY]).

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 « Wallix AdminBastion**,** version 3.1.9 avec correctifs de sécurité 3354, 5420 et 5435 **»** 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 CSPN - Cible de sécurité CSPN - Wallix AdminBastion 3.1.9* ; Référence : *CSPN-WAB-3.1.9* ; Version : *1.1* ; Date : *23 avril 2013.*
[RTE]	*Rapport Technique d'Évaluation (RTE) CSPN Wallix AdminBastion ;* Référence : *OPPIDA/CESTI/CSPN_WAB-3.1/RTE/2.0* ; Version : 2.0 ; Date : *4 octobre 2013.*
[SPEC-CRY]	Spécifications des mécanismes cryptographiques *;* Version : *1.9* ; Date : *28 juin 2013.*
[GUIDES]	Guide d'utilisation : *Guide de démarrage rapide ;* *Guide de l'utilisateur ;* Guide d'administration : *Guide d'Administration ;* *Guide d'utilisation de la console d'administration ;* *Guide de configuration et d'exploitation haute disponibilité ;* *Guide d'activation et de désactivation des services ;* *Guide de configuration X509 ;* *Documentation d'installation du patch de sécurité 3354 ;* *Documentation d'installation du patch de sécurité 5420 ;* *Documentation d'installation du patch de sécurité 5435.*

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 http://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 http://www.ssi.gouv.fr/
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.