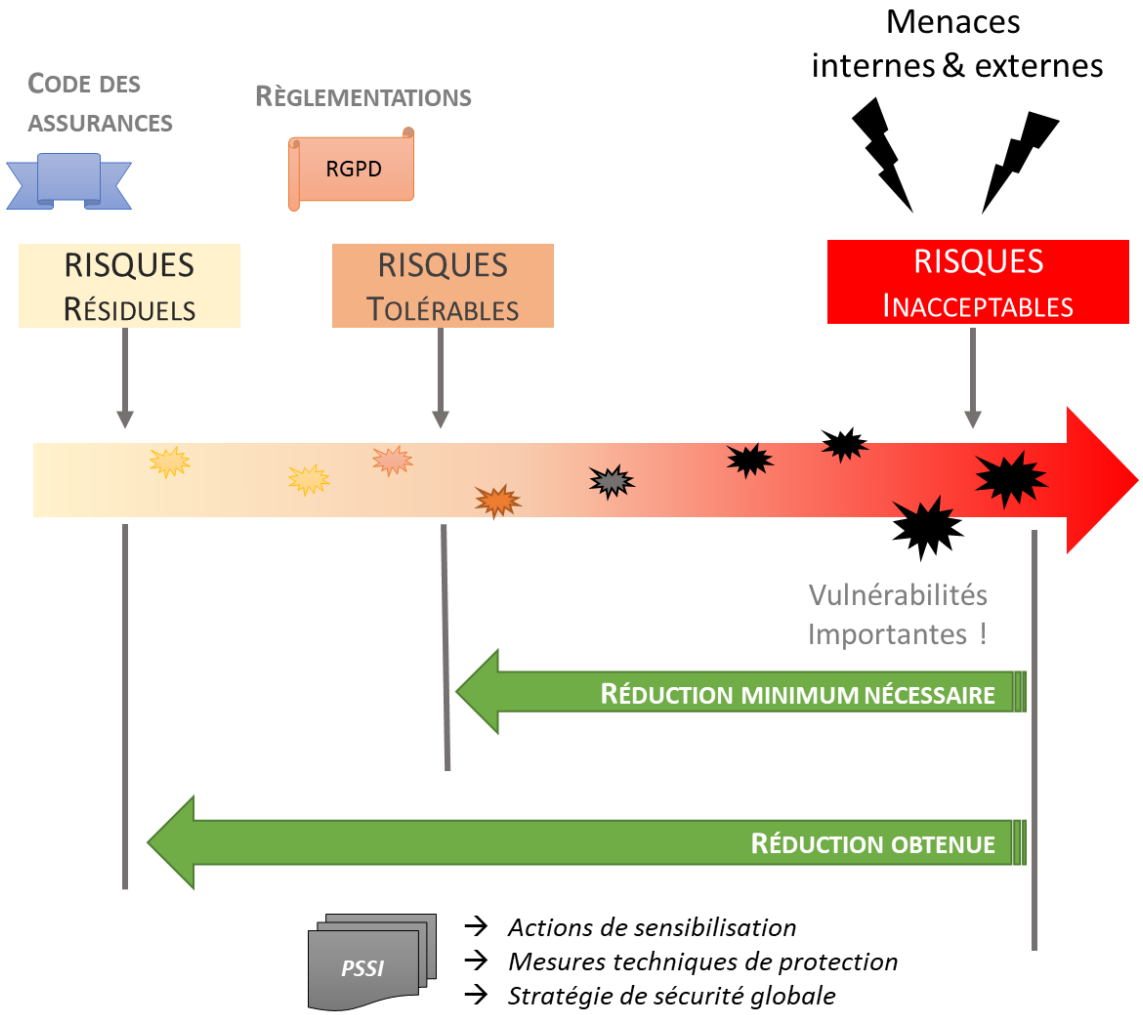
CD24 : HOMOLOGATION ET AUDIT

Rappel – SSI : Appréhender les risques et actions réalisées



T **Homologation technique**

\+

S **Homologation sécurité**

Le CCSC a pour vocation :

- D'assurer un premier cadre de sécurité du SI ;
- D'assurer la sécurisation des données en amont du projet (Privacy By Design) ;
- D'intégrer la sécurité en amont (Security By Design)
- De prendre en compte les 2 types d'hébergements :
  - On Premise = principe d'homologation technique
  - Cloud = étude technique sur la base du Plan d'Assurance Sécurité

SOMMAIRE CCSC

1. INTRODUCTION 3
2. POLITIQUES DE SECURITE 3
3. CONTROLES ET AUDITS 3
4. DOCUMENTATIONS 3
5. MAINTIEN EN CONDITION DE SECURITE 4
6. GESTION ET MESURE DE LA SECURITE 4
7. HEBERGEMENT : SAUVEGARDES 5
8. HEBERGEMENT : LOCALISATION DES DONNEES 5
9. REVERSIBILITE ET PORTABILITE DES DONNEES 5
10. SIGNALEMENTS DE FAILLE DE SECURITE 6
11. SOUS-TRAITANCE 6
12. TELEMAINTENANCE 6
13. ETATS DE L'ART 6
14. RGPD 6

POUR TOUS LES DÉVELOPPEMENTS INTERNES - LES CAHIERS DES CHARGES – LES ÉVOLUTIONS APPLICATIVES
AVANT LA MISE EN PRODUCTION, NOUS DEVONS APPLIQUER L'HOMOLOGATION TECHNIQUE CI-DESSOUS :

HOMOLOGATION TECHNIQUE

- J'installe l'antivirus, l'EDR et le configure
- Je supervise et assure la traçabilité
- Je chiffre et sécurise la communication entre les utilisateurs et l'application
- J'utilise uniquement l'identité numérique centralisée
- J'applique une stratégie de sauvegarde adaptée (si externalisation je vérifie le contrat de service)
- J'identifie les interfaces et les interopérabilités avec d'autres applications
- J'identifie et sécurise toutes les bases de données (type, port, sauvegardes…)
- Je n'autorise que les flux strictement nécessaires au fonctionnement de l'application
- Je connais et note les comptes techniques/services et les droits affectés
- Je valide le cycle de vie des utilisateurs (arrivée, départs, changement…)
- J'automatise et centralise dans l'ordonnanceur
- J'applique les mesures de durcissement : mot de passe par défaut, scans de vulnérabilités, coffre-fort de mdp…)

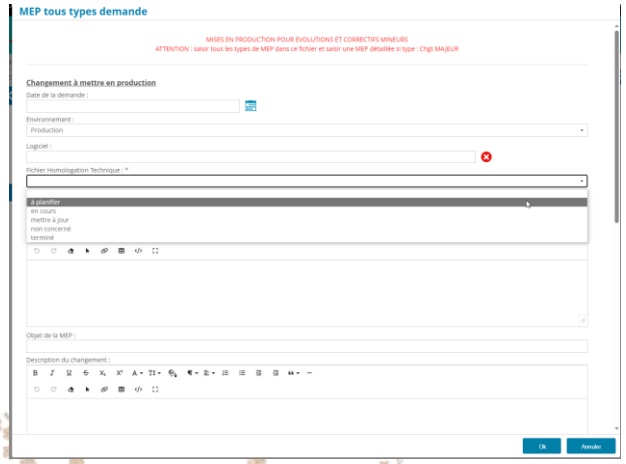
TOUS LES INTERVENANTS DANS LE PROJET DOIVENT REMPLIR LEUR PARTIE

Table des matières

1 DESCRIPTION DU SYSTEME 3
1.1 DESCRIPTION DU SYSTEME 3
1.1.1 URL D'ACCES A L'APPLICATION 3
2 QUALIFICATION DES BESOINS EN SECURITE METIER (DICT) 3
3 SECURITE DU SYSTEME D'INFORMATION 3
3.1 ENVIRONNEMENT SYSTEME 3
3.1.1 SERVEURS 3
3.1.2 INSTALLATION ANTIVIRUS 3
3.1.3 MISE EN PLACE DE LA SUPERVISION 4
3.1.4 STOCKAGE 4
3.1.5 SAUVEGARDES 4
3.1.6 TACHES ORDONNANCEUR 4
3.1.7 RELANCE DES SERVEURS 4
3.2 ENVIRONNEMENT BASES DE DONNEES 4
3.2.1 IDENTIFICATION BASE DE DONNEES 4
3.3 ENVIRONNEMENT RESEAUX 5
3.3.1 PARE FEU FORTINET 5
3.3.2 ADC NETSCALER 5
3.4 AUTHENTIFICATION DES UTILISATEURS DE L'APPLICATION 6
3.4.1 TYPE D'AUTHENTIFICATION 6
3.4.2 COMPTES DE SERVICE ASSOCIES 6
3.4.3 GESTION DES HABILITATIONS 6
3.4.4 PROCEDURES DES ARRIVEES ET DEPARTS DES UTILISATEURS DE L'APPLICATION 6
3.5 INTERFACE ENTRE APPLICATIONS 7
3.5.1 INTERFACES ENTRANTES 7
3.5.2 INTERFACES SORTANTES 7
3.6 SCRIPTS - UTILITAIRES - BATCHS 7
3.7 GESTION DE PROJET ET DES ACCES 7
3.7.1 RESPONSABILITES CD24 7
3.7.2 RESPONSABILITES EDITEUR 7
3.7.3 ACCES A DISTANCE DES PRESTATAIRES 8
3.8 DURCISSEMENT DE CONFIGURATION 8

A remplir et/ou à compléter

- Tous les nouveaux projets
- Evolutions de l'application
  - Patchs mineurs
  - Patchs majeurs
  - Changements infra
  - Ajouts d'interfaces
  - Taches ordonnanceurs
  - …
- Avant toutes MEP



Pas de dossier d'homologation pas de MEP

Doit se faire en amont de la mise en place du socle technique
En cas de marché : après la réunion de lancement du projet
Sur un développement interne : au moment de la réunion de lancement avec les chefs de projet métiers

Objectifs :

- Description du projet et des différents participants / intervenants
- Identification du type d'information traitées et avec quels moyens
- Lien avec le RGPD et la durée de conservation des données
- Identification du niveau de sécurité du nouveau projet
- Mettre les mesures de sécurité adaptées
- Décrire le mode dégradé en cas d'indisponibilité de l'application

DOSSIERS INTEGRATION SECURITE DANS LES PROJETS
MENU

- 1 . DESCRIPTION DU PROJET
- 2 . FLUX DE DONNEES ENTRE APPLICATIONS
- 3 . BESOIN : DISPONIBILITE - INTEGRITE - CONFIDENTIALITE
- 4 . ANALYSE DES RISQUES
- 5 . MESURES DE SECURITE
- 6 . RESULTATS

Guide d'utilisation

1 . Description : partie à renseigner par le chef de projet DSIN

2 . flux de données entre applications: partie à renseigner par le chef de projet DSIN et le(s) développeur(s)

3 . Besoin en DIC : partie à renseigner par le chef de projet métier avec l'accompagnement du chef de projet DSIN

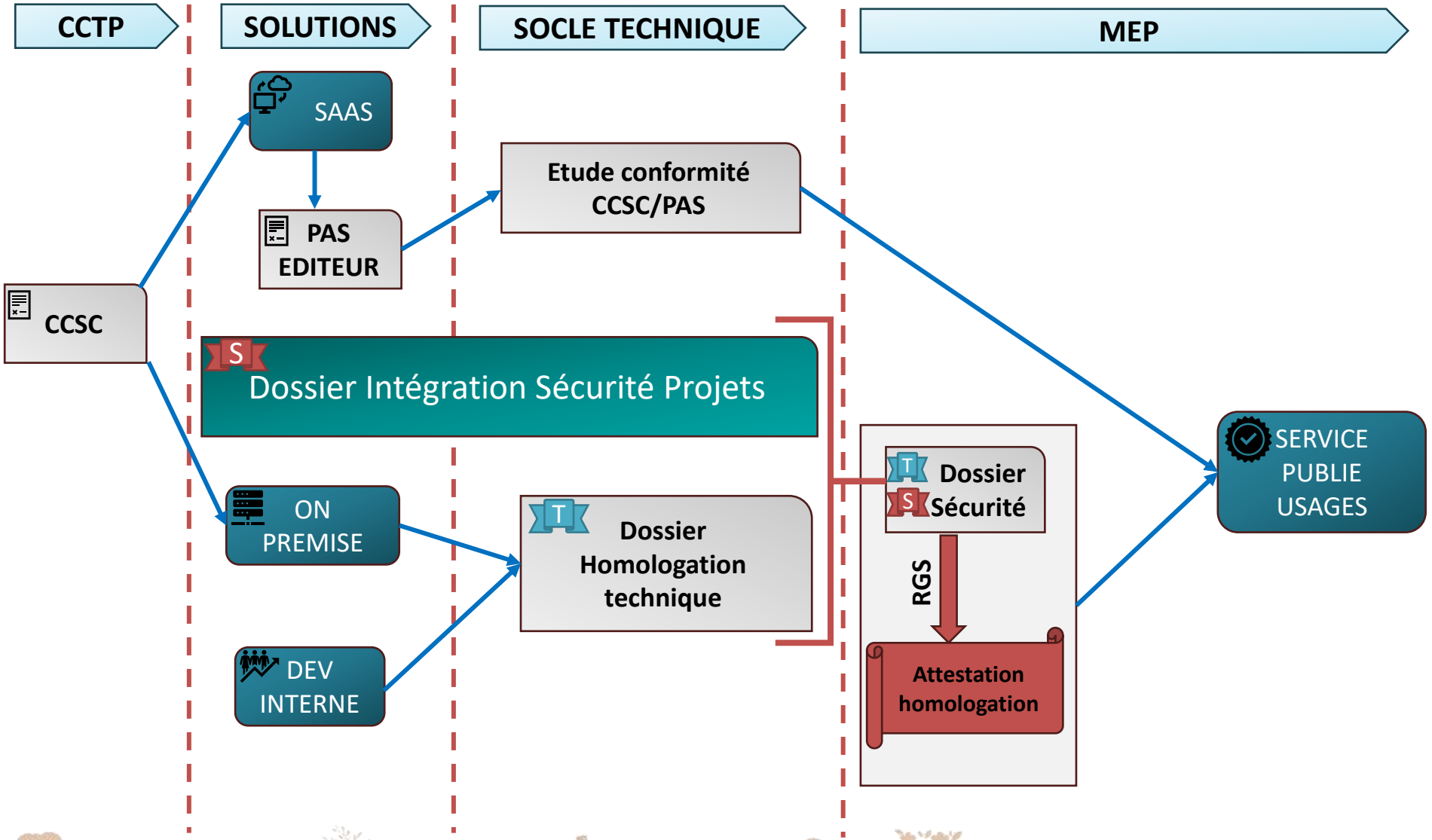
4 . Analyse des risques: partie à renseigner par le chef de projet métier avec l'accompagnement du chef de projet DSIN

5 . Mesures de la sécurité : à renseigner par le RSSI avec le chef de projet DSIN et l'équipe infrastructure

6 . Résultats : en fonction des réponses des points précédents le RSSI va identifier un niveau de criticité de l'application et identifier des mesures complémentaires si nécessaire

APPLICATIONS	Dispo 1 heure	Dispo 4 heures	Dispo 1 jour	Dispo 3 jours	Dispo 14 jours	Défaut d'intégrité	Confidentialité	Mode Dégradé
OPENSUB	Faible	Faible	Faible	Important	Très Important	Très Important	Confidentiel	Système D

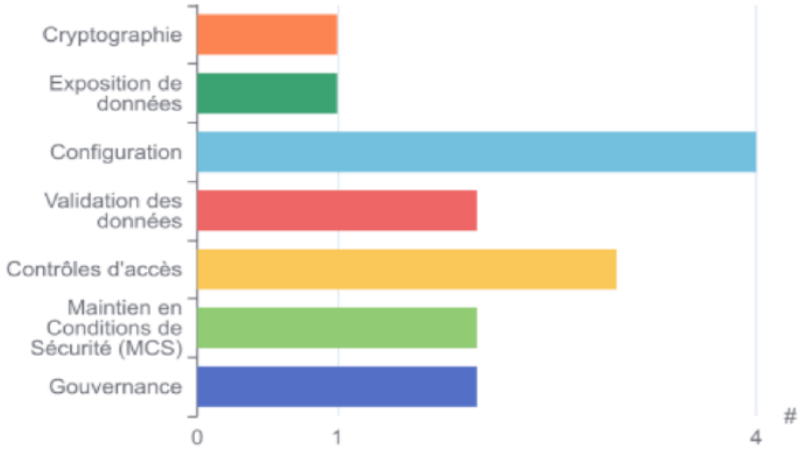
LE PRINCIPE EN SYNTHÈSE POUR SERVICE AUX USAGERS



AUDIT TECHNIQUE : TEST D'INTRUSION EXTERNE

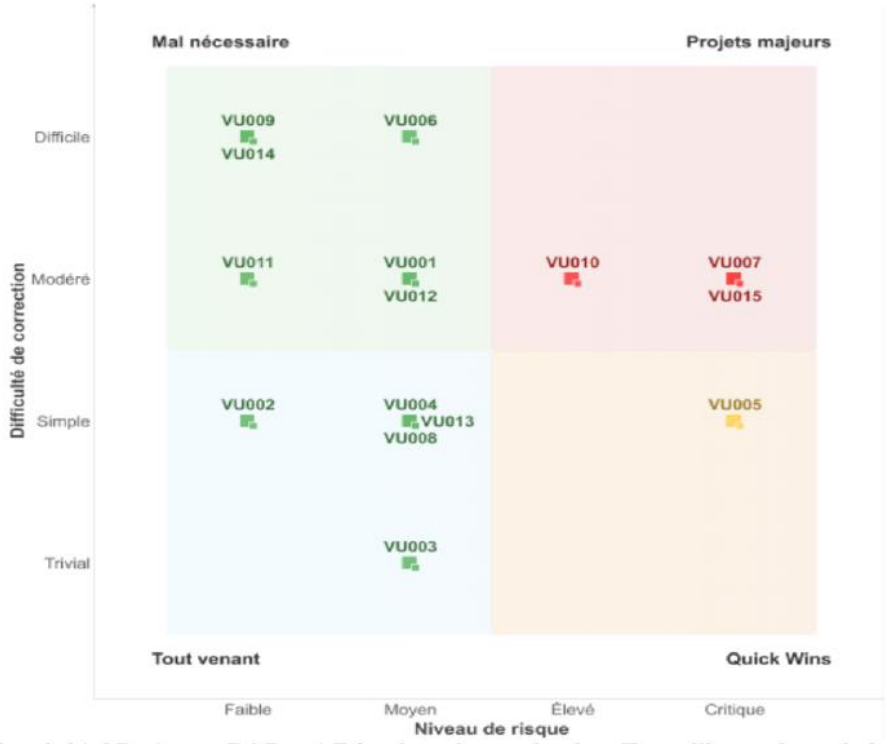
- **Objectifs** : évaluer le risque lié à l'offensive d'un attaquant depuis l'extèrieur et identifier les éventuelles failles et/ou vulnérabilités
- **Champs d'intervention** : audit en boite grise : les auditeurs bénéficiaient de compte d'accès ! L'attaque simulée est celle d'un acteur malveillant qui cible le CD24.

RÉSULTATS DE L'AUDIT PAR CATEGORIE



VULNERABILITES IDENTIFIEES

Référence	Criticité	Vulnérabilité
VU005	Critique	Utilisation de mot de passe par défaut
VU007	Critique	Utilisation de composants vulnérables
VU015	Critique	Administrateur de domaine connecté sur un serveur applicatif
VU010	Élevé	Exposition d'interfaces d'administration sur internet
VU003	Moyen	Présence de fichier phpinfo.php
VU004	Moyen	Présence de fichier sensible dans l'arborescence du serveur
VU008	Moyen	Mode debug d'un composant activé
VU013	Moyen	Fonctionnalité Cron de Wordpress activée
VU001	Moyen	Open Redirect



Quick wins : actions permettant d'avoir un gain rapide de sécurité avec un effort limité;

Projets majeurs : actions prioritaires, mais avec un cout significatif de mise en œuvre (ressources, délais, etc…)

Tout venant : actions à traiter dans un second temps, en fonction de la disponibilité laissée par les tâches plus prioritaires ;

Mal nécessaire : A mettre en œuvre une fois que toutes les autres actions ont été réalisées.

VU005 - Utilisation de mot de passe par défaut — Critique

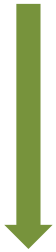
Il est recommandé de changer systématiquement les mots de passe par défaut définis par l'éditeur par des mots de passe forts, aléatoires et à usage unique.

Difficultés
Obligation du changement des mots de passe par les éditeurs

→ Mesure intégrée au CCSC

VU015 - Administrateur de domaine connecté sur un serveur applicatif — Critique

Un administrateur du domaine était connecté sur un serveur web.
Cet administrateur de domaine laisse des traces sur le serveur, et en particulier des informations d'authentification se trouvent en mémoire du processus LSASS (Local Security Authority Subsystem Service).



Rappel des règles et des bonnes pratiques des admin du SI
Charte des Administrateurs

VU007 - Utilisation de composants vulnérables — Critique

Des serveurs exposés sur internet utilisent des composants affectés par des vulnérabilités connues.

Ancienne version d'Apache
Ancienne version de CMS Spip – Lien Docker
Ancienne version de Worpress
Ancienne version de JasperReport
…
avec CVE associées

Difficultés
Sites maintenus par les éditeurs
Comment les obliger à mettre à jour.

CCSC et intégration du Maintien en conditions de Sécurité

VULNERABILITES IDENTIFIEES

VU003 - Présence de fichier phpinfo.php — Moyen

Des fichiers `phpinfo.php` sont disponibles sur plusieurs serveurs web, divulguant des informations sensibles sur l'application et le serveur.

VU004 - Présence de fichier sensible dans l'arborescence du serveur — Moyen

Des fichiers sensibles ont été identifiés dans l'arborescence du serveur et sont accessibles aux utilisateurs sans authentification.

Désactivation du listage du contenu des dossiers
blocage des urls par nos reverses proxy

SCAN DE VULNERABILITES

- Pour pallier le contexte budgétaire délicat :
  - Projet de solution OpenSource de scan de vulnérabilité
  - Automatisation des scans sur les urls, les Ips et/ou sous réseaux
- Solution identifiée et implémentée : OPENVAS – Greenbone

Report:Tue, Jan 9, 2024 8:12 AM UTC Done

ID: e8ff8006-bf75-46d9-93b7-ddf2085d9cc2 Created: Tue, Jan 9, 2024 8:12 AM UTC Modified: Tue, Jan 9, 2024 8:53 AM UTC Owner: admin

Information | Results (65 of 152) | Hosts (1 of 1) | Ports (4 of 9) | Applications (29 of 29) | Operating Systems (1 of 1) | CVEs (59 of 59) | Closed CVEs (2343 of 2343) | TLS Certificates (1 of 1) | Error Messages (1 of 1) | User Tags (0)

1 - 65 of 65

Vulnerability	Severity ▼	QoD	Host	Location	Created
Apache Log4j End of Life (EOL) Detection - Windows	10.0 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:26 AM UTC
VMware Spring Framework End of Life (EOL) Detection - Windows	10.0 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:28 AM UTC
Apache Tomcat End of Life (EOL) Detection - Windows	10.0 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:28 AM UTC
Apache Tomcat Multiple Vulnerabilities (Feb 2020) - Windows	9.8 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:28 AM UTC
Apache Log4j 1.x Multiple Vulnerabilities (Windows, Jan 2022) - Version Check	9.8 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:26 AM UTC
Apache Log4j 1.2.x <= 1.2.17 RCE Vulnerability - Windows	9.8 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:26 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %		8009/tcp	Tue, Jan 9, 2024 8:35 AM UTC
Oracle Java SE Security Update (oct2021) 01 - Windows	8.6 (High)	97 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC
Oracle Java SE Security Update (cpuapr2020 - 01) - Linux	8.3 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC
Oracle Java SE Security Updates - 01 - (cpujul2020) - Windows	8.3 (High)	97 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC
Oracle Java SE Security Updates - 03 - (cpujul2020) - Windows	8.3 (High)	97 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC
Oracle Java SE Security Update (cpuapr2020 - 01) - Windows	8.3 (High)	97 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC
Oracle Java SE Security Update (cpujan2020 - 01) - Windows	8.1 (High)	97 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC
Windows IExpress Untrusted Search Path Vulnerability	7.8 (High)	80 %		general/tcp	Tue, Jan 9, 2024 8:27 AM UTC