astorya
solution globale informatique

F-Secure Elements Vulnerability Management

Résumé

ASTORYA_Comp - Rapport_[redacted]_Etat_des_lieux

Détails du rapport

Durée de l'analyse : [redacted]

Rapport créé : [redacted]

Généré par : __NOT_SET__
__NOT_SET__

Table des matières

À propos de ce document

Ce rapport de sécurité a été généré par F-Secure Radar, une solution de gestion des vulnérabilités fournie par F-Secure. Il contient les résultats de l' analyse de sécurité de plusieurs cibles gérées par ASTORYA_Comp. Il inclut notamment les vulnérabilités détectées par le module d'analyse ainsi que des conseils pratiques pour y remédier. En outre, dans la mesure où il divulgue des informations confidentielles, seules les personnes agréées par ASTORYA_Comp sont autorisées à le consulter.

À propos des analyses de risques en sécurité de l'information

Dans le domaine de la sécurité de l'information, une analyse de risques vise à déterminer à tout moment le niveau de sécurité d'un composant. Si, dans le meilleur des cas, une analyse des vulnérabilités est en effet capable de fournir un excellent aperçu du niveau de sécurité d'une cible donnée, elle ne doit jamais constituer l'unique processus garant de la sécurité de l'information.

Comme expliqué, une analyse fournit un aperçu représentatif, mais pas nécessairement exhaustif. Il se peut que des failles et des vulnérabilités visibles au stade de la conception ne soient pas détectées. En d'autres termes, une analyse des vulnérabilités est capable de révéler des problèmes de sécurité, mais ne peut toutefois pas en garantir l'absence totale.

En outre, les techniques d'attaque et de défense sont en constante évolution. Il arrive parfois même qu'une toute nouvelle catégorie de vulnérabilités soit mise à jour. C'est la raison pour laquelle les résultats d'une analyse des vulnérabilités expirent au fil du temps et qu'il est recommandé d'évaluer régulièrement les principales fonctions opérationnelles.

1. Rapport de synthèse

Donner au client un aperçu de l'état de sécurité de son infrastructure informatique.
En fonction des cibles d'analyse sélectionnées et de la configuration de rapport de synthèse décrite ci-dessous, le **niveau de sécurité global des systèmes évalués** est :

Faible

1.1. Portée

La portée de ce rapport couvre l'ensemble des hôtes **75**.

Le tableau suivant indique un sous-ensemble des systèmes les plus vulnérables.

Nom	Cible	Résultats (Modifications entre parenthèses)			
		Elevée	Moyen	Faible	Info
[redacted]	[redacted]	7	48	2	10
[redacted]	[redacted]	5	31	15	33
[redacted]	[redacted]	5	20	9	20
[redacted]	[redacted]	5	20	9	20
[redacted]	[redacted]	3	8	5	13
[redacted]	[redacted]	3	1	4	18
[redacted]	[redacted]	2	24	20	37
[redacted]	[redacted]	1	14	8	13
[redacted]	[redacted]	1	4	4	15
[redacted]	[redacted]	1	0	1	6
[redacted]	[redacted]	1	0	1	5
[redacted]	[redacted]	0	40	30	75
[redacted]	[redacted]	0	10	8	23
[redacted]	[redacted]	0	9	3	14
[redacted]	[redacted]	0	8	4	13
[redacted]	[redacted]	0	6	5	16
[redacted]	[redacted]	0	5	6	11
[redacted]	[redacted]	0	3	5	10
[redacted]	[redacted]	0	1	2	8
[redacted]	[redacted]	0	0	1	3
[redacted]	[redacted]	0	0	0	3
[redacted]	[redacted]	0	0	0	3
[redacted]	[redacted]	0	0	0	3
[redacted]	[redacted]	0	0	0	3
[redacted]	[redacted]	0	0	0	3

La table a été tronquée. Les 50 restants ne seront pas affichés.

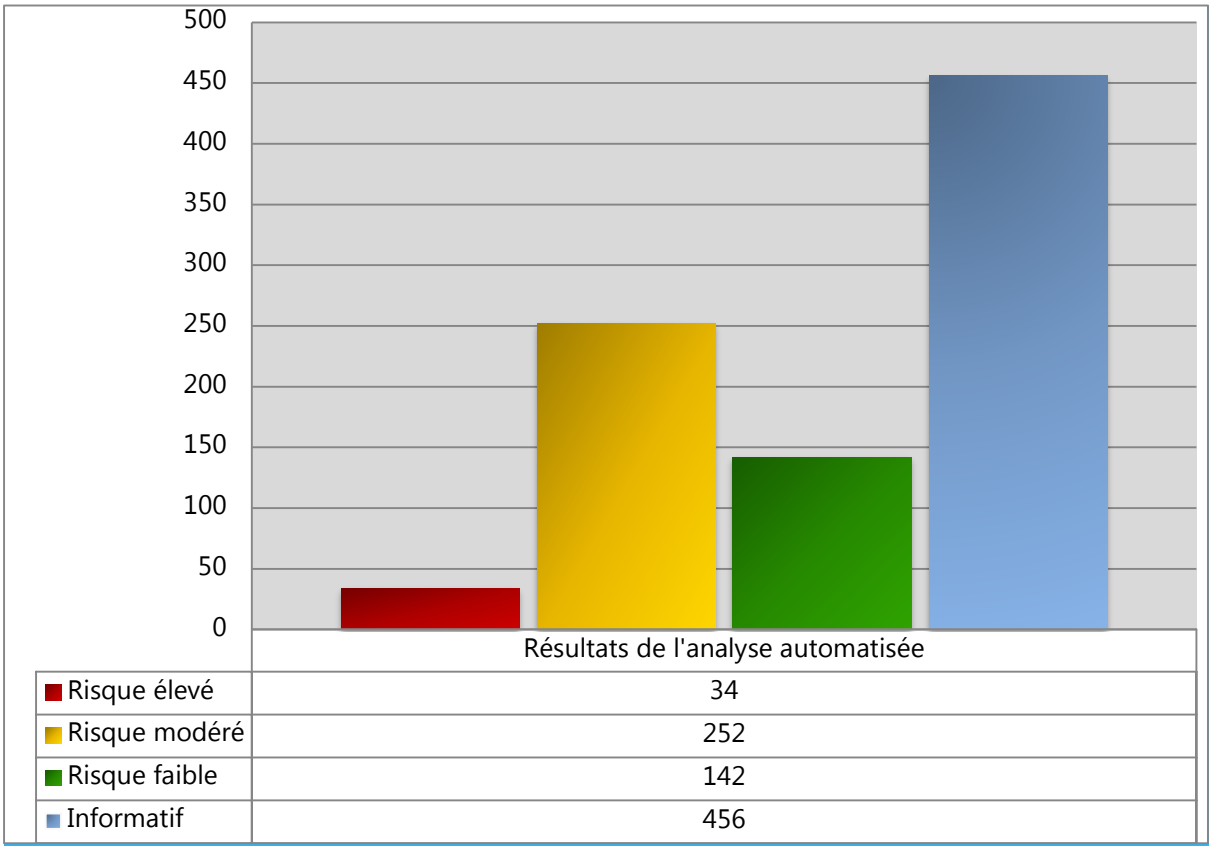
1.2. Options du rapport de synthèse

Pour comprendre le contexte de ce rapport, il est important d'examiner les options décrites ci-dessous. Par exemple, un rapport contenant exclusivement des vulnérabilités à risque élevé doit être interprété différemment d'un rapport qui inclut la totalité des vulnérabilités.

Généralités		
Groupe d'analyses/Cibles d'analyse		
-		
Gravité des vulnérabilités	États des vulnérabilités	Balises de vulnérabilité
☒ Élevé ☒ Moyen ☒ Faible ☒ Résultats à titre informatif	☒ Non Unattended ☒ Non Confirmed ☒ Non Pending ☒ Non Accepted risk ☒ Non PCI compliant ☒ Non Reopened ☒ Non False Positive ☒ Non Duplicate ☒ Non Fixed	-
Options diverses		
☒ Afficher les états de vulnérabilités ☒ Afficher les références externes	☒ Afficher les notes de l'auditeur ☐ Afficher les balises	☒ Afficher l'indicateur de modification
Analyse système		
Catégories de vulnérabilités incluses	Types d'exploits de vulnérabilité	Options diverses
All categoriescatégories	☒ Exploitable localement ☒ Exploitable à distance	☒ Inclure les vulnérabilités potentielles ☐ Inclure uniquement lorsqu'une exploitation publique est disponible
Analyse Web		
Catégories de vulnérabilités incluses		
All categoriescatégories		

1.3. État actuel du système

1.3.1. Nombre total de vulnérabilités



	Résultats de l'analyse automatisée
Risque élevé	34
Risque modéré	252
Risque faible	142
Informatif	456

1.3.2. Statistiques des cibles vulnérables

Analyse de la plateforme	
Nombre total d'hôtes avec des vulnérabilités à risque élevé	11
Nombre total d'hôtes avec des vulnérabilités à risque modéré	17
Nombre total d'hôtes avec des vulnérabilités à risque faible	20
Nombre total de sites avec des résultats informatifs	73
Nombre total d'hôtes	74
Nombre total de vulnérabilités sur les hôtes	428

Analyse Web	
Total number of sites with High vulnerabilities	0
Total number of sites with Medium vulnerabilities	0
Total number of sites with Low vulnerabilities	0

Total number of sites with Informational findings	0
Total number of sites	1
Total number of vulnerabilities on sites	0

1.3.3. Top 10 des cibles les plus vulnérables

Analyse de la plateforme				
Nom	**Cible**	**Résultats**		
		Elevée	**Moyen**	**Faible**
[redacted]	[redacted]	7	48	2
[redacted]	[redacted]	5	31	15
[redacted]	[redacted]	5	20	9
[redacted]	[redacted]	5	20	9
[redacted]	[redacted]	3	8	5
[redacted]	[redacted]	3	1	4
[redacted]	[redacted]	2	24	20
[redacted]	[redacted]	1	14	8
[redacted]	[redacted]	1	4	4
[redacted]	[redacted]	1	0	1

Analyse Web				
Nom	**Cible**	**Résultats**		
		Elevée	**Moyen**	**Faible**
[redacted]	https:/[redacted].com/	0	0	0

1.3.4. Top 3 des vulnérabilités à risque élevé/modéré les plus fréquentes

Analyse de la plateforme	
Instance de vulnérabilité	**Hôtes concernés**
HTTP Response Date is not Synchronised	7
lighttpd before 1.4.54 Integer Overflow Vulnerability	5
End-of-life product: jQuery	3
SSL certificate is not valid	35
Remote server supports TLS 1.0	31
Remote server supports TLS 1.1	30

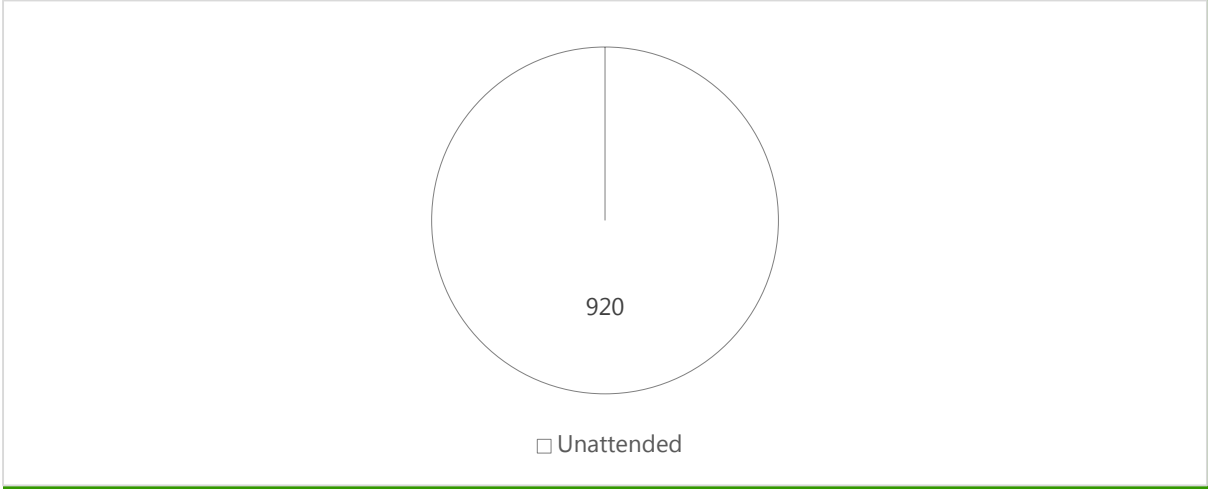
1.3.5. Évaluation de la maturité de SSL/TLS

Problèmes d'implémentation de SSL/TLS	Hôtes concernés
SSL certificate is not valid	35
Remote server supports TLS 1.0	31
Remote server supports TLS 1.1	30
SSL certificate uses SHA1 signature	18
SSL/TLS RC4 Cipher Suites Supported	10
SSL Certificate RSA key length less than 2048 bits	8
SSL Certificate expired	7
Remote server supports SSL 3.0	5
SSL3 POODLE vulnerability	4
SSL supports weak ciphers (56bit / 64bit)	2
SSL Certificate signed using a weak algorithm	1
SSL Certificate signed using MD5 algorithm which is not resistant to collisions	1

1.3.6. État du groupe d'analyses

Nom du groupe d'analyses	Hôtes concernés triés par sécurité		
[redacted]_System	34 (7%)	252 (58%)	142 (33%)
[redacted]_Publique		2 (66%)	1(33%)
[redacted]_WEB	0 (0%)	0 (0%)	0 (0%)

1.3.7. Progression de la gestion des vulnérabilités



2. ANNEXE

2.1. À propos de la méthodologie de test

La complexité des infrastructures étendues et des solutions informatiques modernes conduit à la nécessité d'effectuer des analyses de sécurité à la fois complètes et équilibrées. Pour relever ce défi, F-Secure a développé une méthodologie propriétaire visant à évaluer la sécurité des environnements requis.

En règle générale, le processus d'analyse des vulnérabilités comporte quatre phases distinctes.

2.1.1. Reconnaissance

Cette phase donne un aperçu global de l'environnement cible. L'objectif étant d'identifier les composants et les services présents au sein de l'infrastructure. Les données relatives aux cibles (hôtes, URL, informations d'identification) peuvent être collectées par le biais de divers moyens, tels que des bases de données WHOIS, des DNS incluant des techniques d'intelligence ou encore les entrées émanant du client. Par ailleurs, la cartographie du réseau F-Secure Elements Vulnerability Management fondée sur le scanneur de F-Secure sert à déterminer les systèmes installés sur les réseaux du client.

2.1.2. Énumération

Au cours de cette phase, les données collectées précédemment sont exploitées pour analyser de la façon la plus détaillée possible les composants et services individuels. L'analyse de la plateforme est effectuée au moyen de l'analyse système F-Secure Elements Vulnerability Management, tandis que les applications Web sont quant à elles analysées via l'analyse Web F-Secure Elements Vulnerability Management.

2.1.3. Recherche de vulnérabilités et d'exploitation (facultatif)

Il s'agit d'une phase manuelle et facultative qui met fortement à contribution l'utilisateur de F-Secure Elements Vulnerability Management. En effet, les vulnérabilités identifiées à la phase précédente doivent être vérifiées scrupuleusement afin d'éviter autant que possible les faux positifs et, au contraire, garantir l'obtention de résultats d'une qualité optimale.

2.1.4. Création de rapports

La phase finale correspond à la création de rapports, soit le fait de documenter toutes les vulnérabilités identifiées au cours de l'analyse. Chaque résultat fait l'objet d'une description détaillée incluant l'emplacement exact, les conditions de survenance (complétées par des informations permettant au client de reproduire le résultat), l'évaluation de l'impact sur la sécurité et la solution proposée. L'objectif est de fournir des renseignements précis sur les problèmes de sécurité, tout en indiquant la meilleure façon de les résoudre.

F-Secure Elements Vulnerability Management dispose d'un puissant moteur de création de rapports grâce auquel l'utilisateur final peut personnaliser le contenu des rapports et les télécharger sous différents formats.

2.2. À propos du score CVSS

Chaque résultat figurant dans le rapport se voit attribuer une note numérique (appelée « score ») à l'aide des métriques internationales CVSSv2. L'objectif du système d'évaluation est d'identifier des métriques communes pour les résultats. Le fait de recourir à un système standardisé permet de comparer les résultats entre les différentes affectations. Il convient toutefois de noter que la note numérique n'est fournie qu'à titre d'indicatif et, par conséquent, doit être interprétée en tant que tel. Le système CVSSv2 est fondé sur les métriques de base suivantes :

- Les métriques de vecteur d'accès (Access Vector (AV)), de complexité d'accès (Access Complexity (AC)) et d'authentification (Authentication (Au)) définissent le mode d'accès à la vulnérabilité et si l'existence de conditions supplémentaires est nécessaire en vue de son exploitation.
- Les métriques de confidentialité (Confidentiality (C)), d'intégrité (Integrity (I)) et de disponibilité (Availability (A)) définissent de quelle façon une vulnérabilité exploitée affectera directement un actif informatique.

2.2.1. Niveau de gravité

En outre, le système CVSSv2 classe le niveau de gravité selon trois catégories différentes : Élevé, Modéré ou Faible. Ce classement qualitatif est établi à partir des notes numériques (scores).

Gravité CVSS score	**Faible** 0.0 – 3.9	**Moyen** 4.0 – 6.9	**Elevée** 7.0 – 10.0

2.3. Niveau de sécurité

Un niveau de sécurité est défini sur la base de la vulnérabilité la plus grave détectée au cours de l'analyse. Pour en savoir plus, reportez-vous à l'illustration et à la description ci-dessous.

Vulnérabilitée la plus grave détectée

Niveau de sécurité	Aucune vulnérabilité	Faible	Moyen	Elevée
Très élevé	●			
Elevée		●		
Moyen			●	
Faible				●

- Un niveau de sécurité très élevé résulte d'une analyse n'ayant détecté aucune vulnérabilité.
- Un niveau de sécurité élevé résulte d'une analyse n'ayant détecté que des vulnérabilités à risque faible.
- Un niveau de sécurité modéré résulte d'une analyse ayant détecté des vulnérabilités à risque moyen.
- Un niveau de sécurité faible résulte d'une analyse ayant détecté des vulnérabilités à risque élevé.

3. Tableau Récapitulatif

Nom Equipement	Type	Adresse IP	Vulénrabilité	Risque	Correctif des vulnérabilités	Responsable
Borne de recharge électrique [redacted]	Microcontrôleur Raspberry Pi	192.168[redacted]	7	Attaque DOS qui va faire crasher le logiciel de contrôle de la borne et peut être une partie du réseau privé. Entrée possible dans le réseau privé.	2 failles : Mettre à jour Apache Tomcat vers une version stable (9.0.31 minimum). Mettre à jour la bibliothèque jQuery. 4 failles : Mettre à jour le serveur Apache vers une version stable (2.4.26 minimum).	https://www.[redacted].com/fr/rapport-de-securite
My IC WEB Office IPBr Telecom [redacted]	Téléphonie	192.168[redacted]	5	Attaque DOS qui va faire crasher le service téléphonique	5 failles : Mettre à jour le serveur Lighttpd	Votre fournisseur téléphonique professionnel ou [redacted]
Borne Wifi [redacted]	Routeur	192.168[redacted]	5	Erreur dans les mises à jour, sauvegardes ou l'analyse d'une attaque.	Mettre à jour le logiciel serveur SSH (version 2016,74 minimum) Mettre à jour la bibliothèque jQuery. 3 Failles : sur les ports 80/443/4343, Synchroniser la date et l'heure (Actuellement : 08/04/1970)	L'opérateur qui à installer votre réseaux Wi-Fi ou votre opérateur internet.
Borne Wifi [redacted]	Routeur	192.168[redacted]	5	Erreur dans les mises à jour, sauvegardes ou l'analyse d'une attaque.	Mettre à jour le logiciel serveur SSH (version 2016,74 minimum) Mettre à jour la bibliothèque jQuery. 3 Failles : Synchroniser la date et l'heure (Actuellement : 08/04/1970)	L'opérateur qui à installer votre réseaux Wi-Fi ou votre opérateur internet.

Nom Equipement	Type	Adresse IP	Vulénrabilité	Risque	Correctif des vulnérabilités	Responsable
[redacted]	Serveur	192.168[redacted]	3	Plus de Mise à jour de sécurité. Failles publiques.	3 Failles : Mettre à jour Jetty	Service informatique ou le prestataire chargé de la maintenance
[redacted]	Imprimante Konica	192.168[redacted]	3	Lecture des informations relatives à l'imprimante	Mettre à jour SNMP vers la version 3 ou changer le nom commun par défaut Désactiver les sessions par défaut (NULL) Désactiver l'accès aux réseaux et fichiers partagés par les inconnus	Service informatique ou Support Constructeur
SRV-APPLI	Serveur	192.168[redacted]	2	Gain des droits administrateurs et Vers informatiques comme Voyager Alpha Force et Spida	2 Failles : Ajouter un MDP au compte "SA" des SQL Serveurs	Service informatique
[redacted]	Imprimante Sharp	192.168[redacted]	1	Lecture des informations relatives à l'imprimante	Mettre à jour SNMP vers la version 3 ou changer le nom commun par défaut ("public")	Service informatique ou Support Constructeur
Epson	Imprimante Epson	192.168[redacted]	1	Lecture des informations relatives à l'imprimante	Mettre à jour SNMP vers la version 3 ou changer le nom commun par défaut ("public")	Service informatique ou Support Constructeur
[redacted]	Ordinateur	192.168[redacted]	1	Plus de Mise à jour de sécurité. Failles publiques.	Mettre à jour le system d'exploitation vers un Windows10	Service informatique
HP	Ordinateur	192.168[redacted]	1	Erreur dans les mises à jour, sauvegardes ou l'analyse d'une attaque.	Synchroniser la date et l'heure (Actuellement :15/02/2001)	Service informatique