KEYSTONE.

USTHB

22/06/2025

Nom du projet : Soutenance

ID du scan : 68576255a1005d12c3f7bda3

Domaine cible : interieur.gov.dz

Date : 22/06/2025

INFORMATIONS SUR LE DOMAINE

Registrar : Non renseigné

Date de création : Non renseignée

Date d'expiration : Non renseignée

Serveurs DNS :

Statut : Inconnu

Email(s) :

ENREGISTREMENTS DNS

A: 196.20.110.179

AAAA: [VIDE]

MX: 10 mx1.interieur.gov.dz., 20 mx2.interieur.gov.dz.

NS: ns1.wissal.dz., ns2.wissal.dz.

TXT: "v=spf1 ip4:193.194.95.132/32 ip4:196.20.110.180/32 -all"

CNAME: [VIDE]

SOUS-DOMAINES DÉTECTÉS

Sous-domaine	Adresse(s) IP
capacitepc.interieur.gov.dz	196.20.73.196, 193.194.95.138
demande12s.interieur.gov.dz	193.194.95.130, 196.20.110.178
etatcivil.interieur.gov.dz	196.20.73.194
interieur.gov.dz	196.20.110.179

Sous-domaine	Adresse(s) IP
mail1.interieur.gov.dz	193.194.95.130
macnibe.interieur.gov.dz	196.20.110.181, 193.194.95.133
mail2.interieur.gov.dz	196.20.110.178
nechki.interieur.gov.dz	193.194.95.140, 196.20.73.198
mx1.interieur.gov.dz	196.20.110.180
mx2.interieur.gov.dz	193.194.95.132
passeport.interieur.gov.dz	196.20.110.181, 193.194.95.133
services.interieur.gov.dz	196.20.110.179, 193.194.95.131
prestations.interieur.gov.dz	196.20.73.197, 193.194.95.139
pelerinage.interieur.gov.dz	196.20.73.193
www.interieur.gov.dz	196.20.110.179
webmail.interieur.gov.dz	196.20.110.180, 193.194.95.132

Adresse IP : 196.20.110.179

Domaine(s) associé(s) : interieur.gov.dz, services.interieur.gov.dz, www.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	N/A	False	—	**Basse**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

1 - Risques potentiels :
- Exposition de services web sans protection
- Potentiellement vulnérables aux attaques par injection SQL ou XSS

2 - Mesures de sécurité préventives :
- Application d'un pare-feu web pour bloquer les attaques par injection SQL et XSS
- Utilisation de frameworks de développement web sécurisés pour réduire les risques d'attaques

Adresse IP : 196.20.73.196

Domaine(s) associé(s) : capacitepc.interieur.gov.dz

Services détectés : 0

Aucun service détecté pour cette IP.

Recommandations

Aucune recommandation n’a été générée.

Adresse IP : 193.194.95.138

Domaine(s) associé(s) : capacitepc.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	**Haute**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-site Scripting (XSS) dans Apache Struts 1.x. Un attaquant peut injecter du code malveillant dans une application web utilisant Apache Struts 1.x via des paramètres HTTP.
- Recommandation : Mettre à jour Apache Struts à la version 1.3.10 ou supérieure pour résoudre la vulnérabilité.

CVE-2017-9788 :
- Description : Vulnérabilité de type Cross-site Scripting (XSS) dans Apache Struts 2.x. Un attaquant peut injecter du code malveillant dans une application web utilisant Apache Struts 2.x via des paramètres HTTP.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.16 ou supérieure pour résoudre la vulnérabilité.

CVE-2017-9798 :
- Description : Vulnérabilité de type Cross-site Scripting (XSS) dans Apache Struts 2.x. Un attaquant

peut injecter du code malveillant dans une application web utilisant Apache Struts 2.x via des paramètres HTTP.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.16 ou supérieure pour résoudre la vulnérabilité.

Adresse IP : 193.194.95.130

Domaine(s) associé(s) : demande12s.interieur.gov.dz, mail1.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	**Haute**
443	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	False	—	**Basse**

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 1.x, qui permet à un attaquant d'injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la version 1.3.10 ou supérieure pour corriger la vulnérabilité.

CVE-2017-9788 :
- Description : Vulnérabilité de type Remote Code Execution (RCE) dans Apache Struts 2.x, qui permet à un attaquant de s'exécuter en tant qu'utilisateur système.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.16 ou supérieure pour corriger la vulnérabilité.

CVE-2017-9798 :
- Description : Vulnérabilité de type Remote Code Execution (RCE) dans Apache Struts 2.x, qui permet à un attaquant de s'exécuter en tant qu'utilisateur système.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.16 ou supérieure pour corriger la vulnérabilité.

Adresse IP : 196.20.110.178

Domaine(s) associé(s) : demande12s.interieur.gov.dz, mail2.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	**Haute**
443	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	False	—	**Basse**

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-Site Scripting (XSS) dans le service HTTP sur le port 80. Cette vulnérabilité peut permettre à un attaquant de injecter du code malveillant dans une page web, ce qui peut entraîner des actions malveillantes telles que l'obtention d'informations sensibles, la modification de données ou la détournement de sessions utilisateur.
- Recommandation : Mettre à jour le logiciel web concerné pour corriger la vulnérabilité. Si cela n'est pas possible immédiatement, il est recommandé d'appliquer des mesures de protection supplémentaires telles que l'utilisation de filtres de sortie pour empêcher l'injection de code malveillant.

CVE-2017-9788 :
- Description : Vulnérabilité de type Cross-Site Request Forgery (CSRF) dans le service HTTP sur le port 80. Cette vulnérabilité peut permettre à un attaquant de forcer un utilisateur authentifié à effectuer des actions malveillantes sur le site web, telles que la modification de ses informations personnelles ou la détournement de ses sessions.
- Recommandation : Mettre à jour le logiciel web concerné pour corriger la vulnérabilité. Si cela n'est pas possible immédiatement, il est recommandé d'appliquer des mesures de protection supplémentaires telles que l'utilisation de tokens de sécurité pour empêcher les attaques CSRF.

CVE-2017-9798 :
- Description : Vulnérabilité de type Injection SQL (SQL Injection) dans le service HTTP sur le port 80. Cette vulnérabilité peut permettre à un attaquant de manipuler les données de la base de données du site web, telles que l'obtention d'informations sensibles, la modification de données ou la détournement de sessions utilisateur.
- Recommandation : Mettre à jour le logiciel web concerné pour corriger la vulnérabilité. Si cela n'est pas possible immédiatement, il est recommandé d'appliquer des mesures de protection supplémentaires telles que l'utilisation de préparation paramétrée pour empêcher les attaques SQL Injection.

Adresse IP : 196.20.73.194

Domaine(s) associé(s) : etatcivil.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	N/A	False	—	**Basse**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

1 - Risques potentiels :
- Exposition de services web sans protection

2 - Mesures de sécurité préventives :
- Configurer un pare-feu pour bloquer les ports non nécessaires
- Installer un système de détection intrusion pour les ports ouverts
- Configurer les services web avec des règles de sécurité strictes

Adresse IP : 196.20.110.181

Domaine(s) associé(s) : macnibe.interieur.gov.dz, passeport.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	**Haute**
443	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	False	—	**Basse**

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 1.x. Un attaquant peut injecter du code malveillant dans une page web, ce qui peut permettre d'exécuter des actions malveillantes sur le navigateur du visiteur.

- Recommandation : Mettre à jour Apache Struts à la version 1.3.10 ou supérieure pour résoudre la vulnérabilité.

CVE-2017-9788 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x. Un attaquant peut injecter du code malveillant dans une page web, ce qui peut permettre d'exécuter des actions malveillantes sur le navigateur du visiteur.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.18 ou supérieure pour résoudre la vulnérabilité.

CVE-2017-9798 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x. Un attaquant peut injecter du code malveillant dans une page web, ce qui peut permettre d'exécuter des actions malveillantes sur le navigateur du visiteur.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.18 ou supérieure pour résoudre la vulnérabilité.

Adresse IP : 193.194.95.133

Domaine(s) associé(s) : macnibe.interieur.gov.dz, passeport.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	**Haute**
443	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	False	—	**Basse**

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 1.x. Un attaquant peut injecter du code malveillant dans une page web, ce qui peut entraîner des actions malveillantes sur le navigateur du visiteur.
- Recommandation : Mettre à jour Apache Struts à la version 1.3.10 ou supérieure pour corriger la vulnérabilité.

CVE-2017-9788 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x. Un attaquant

peut injecter du code malveillant dans une page web, ce qui peut entraîner des actions malveillantes sur le navigateur du visiteur.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.16 ou supérieure pour corriger la vulnérabilité.

CVE-2017-9798 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x. Un attaquant peut injecter du code malveillant dans une page web, ce qui peut entraîner des actions malveillantes sur le navigateur du visiteur.
- Recommandation : Mettre à jour Apache Struts à la version 2.5.16 ou supérieure pour corriger la vulnérabilité.

Adresse IP : 193.194.95.140

Domaine(s) associé(s) : nechki.interieur.gov.dz

Services détectés : 0

Aucun service détecté pour cette IP.

Recommandations

Aucune recommandation n’a été générée.

Adresse IP : 196.20.73.198

Domaine(s) associé(s) : nechki.interieur.gov.dz

Services détectés : 0

Aucun service détecté pour cette IP.

Recommandations

Aucune recommandation n’a été générée.

Adresse IP : 196.20.110.180

Domaine(s) associé(s) : mx1.interieur.gov.dz, webmail.interieur.gov.dz

Services détectés : 3

Port	Technologie	Version	Vulnérable	CVE	Criticité
25	smtp	FortiMail smtpd (time zone: +0100)	False	—	Basse
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	Haute
443	ssl/https	N/A	False	—	Basse

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 1.x, qui permet à un attaquant de injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la dernière version stable pour résoudre la vulnérabilité.

CVE-2017-9788 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x, qui permet à un attaquant de injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la dernière version stable pour résoudre la vulnérabilité.

CVE-2017-9798 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x, qui permet à un attaquant de injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la dernière version stable pour résoudre la vulnérabilité.

Adresse IP : 193.194.95.132

Domaine(s) associé(s) : mx2.interieur.gov.dz, webmail.interieur.gov.dz

Services détectés : 3

Port	Technologie	Version	Vulnérable	CVE	Criticité
25	smtp	FortiMail smtpd (time zone: +0100)	False	—	Basse

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	True	CVE-2004-0174, CVE-2017-9788, CVE-2017-9798	**Haute**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

CVE-2004-0174 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 1.x, qui permet à un attaquant de injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la dernière version stable pour résoudre la vulnérabilité.

CVE-2017-9788 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x, qui permet à un attaquant de injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la dernière version stable pour résoudre la vulnérabilité.

CVE-2017-9798 :
- Description : Vulnérabilité de type Cross-site scripting (XSS) dans Apache Struts 2.x, qui permet à un attaquant de injecter du code malveillant dans une page web.
- Recommandation : Mettre à jour Apache Struts à la dernière version stable pour résoudre la vulnérabilité.

Adresse IP : 193.194.95.131

Domaine(s) associé(s) : services.interieur.gov.dz

Services détectés : 0

Aucun service détecté pour cette IP.

Recommandations

Aucune recommandation n’a été générée.

Adresse IP : 196.20.73.197

Domaine(s) associé(s) : prestations.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	N/A	False	—	**Basse**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

1 - Risques potentiels :
- Exposition des services web (http et https) sans validation des certificats SSL/TLS
- Potentiellement vulnérable à des attaques de man-in-the-middle

2 - Mesures de sécurité préventives :
- Vérifier la validation des certificats SSL/TLS pour les services web
- Utiliser des solutions de sécurité tels que ModSecurity ou Fail2Ban pour protéger les services web contre les attaques

Adresse IP : 193.194.95.139

Domaine(s) associé(s) : prestations.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	N/A	False	—	**Basse**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

1 - Risques potentiels :
- Exposition de services web sans protection HTTPS
- Potentiellement vulnérable à des attaques de man-in-the-middle

2 - Mesures de sécurité préventives :
- Configurer les services web pour utiliser HTTPS
- Utiliser des certificats valides pour garantir l'authenticité et la confidentialité des communications

Adresse IP : 196.20.73.193

Domaine(s) associé(s) : pelerinage.interieur.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	N/A	False	—	**Basse**
443	ssl/https	N/A	False	—	**Basse**

Recommandations

1 - Risques potentiels :
- Exposition de services web sans protection HTTPS

2 - Mesures de sécurité préventives :
- Configurer les services web pour utiliser HTTPS
- Installer un certificat SSL valide pour les services web