KEYSTONE.

MIRA

21/06/2025

Nom du projet : MIRA

ID du scan : 6855fa33fd24df53d25c6e58

Domaine cible : mta.gov.dz

Date : 21/06/2025

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: Aucun enregistrement trouvé.

AAAA: Aucun enregistrement trouvé.

MX: Aucun enregistrement trouvé.

NS: Aucun enregistrement trouvé.

TXT: Aucun enregistrement trouvé.

CNAME: Aucun enregistrement trouvé.

SOUS-DOMAINES DÉTECTÉS

Sous-domaine	Adresse(s) IP
alger.mta.gov.dz	197.112.10.60
ain-defla.mta.gov.dz	197.112.10.60
ain-temouchent.mta.gov.dz	197.112.10.60
batna.mta.gov.dz	197.112.10.60

Sous-domaine	Adresse(s) IP
beni-abbes.mta.gov.dz	197.112.10.60
chlef.mta.gov.dz	197.112.10.60
bordj-bou-arreridj.mta.gov.dz	197.112.10.60
biskra.mta.gov.dz	197.112.10.60
constantine.mta.gov.dz	197.112.10.60
djelfa.mta.gov.dz	197.112.10.60
djanet.mta.gov.dz	197.112.10.60
el-meniaa.mta.gov.dz	197.112.10.60
el-tarf.mta.gov.dz	197.112.10.60
ghardaia.mta.gov.dz	197.112.10.60
in-guezzam.mta.gov.dz	197.112.10.60
in-salah.mta.gov.dz	197.112.10.60
khenchela.mta.gov.dz	197.112.10.60
mail.mta.gov.dz	197.112.0.130
mta.gov.dz	197.112.125.117
ouled-djellal.mta.gov.dz	197.112.10.60
portail.mta.gov.dz	197.112.0.40
medea.mta.gov.dz	197.112.10.60
oum-el-bouaghi.mta.gov.dz	197.112.10.60
relizane.mta.gov.dz	197.112.10.60
setif.mta.gov.dz	197.112.10.60
sidi-bel-abbes.mta.gov.dz	197.112.10.60
timimoun.mta.gov.dz	197.112.10.60
tizi-ouzou.mta.gov.dz	197.112.10.60
skikda.mta.gov.dz	197.112.10.60
www.mta.gov.dz	197.112.125.117

Adresse IP : 197.112.125.117

Domaine(s) associé(s) : mta.gov.dz, www.mta.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 authentification ni restriction d'accès

2 - Mesures de sécurité préventives :
- Configurer des authentifications et restrictions d'accès aux services web

Adresse IP : 197.112.10.60

Domaine(s) associé(s) : alger.mta.gov.dz, ain-defla.mta.gov.dz, ain-temouchent.mta.gov.dz, batna.mta.gov.dz, beni-abbes.mta.gov.dz, chlef.mta.gov.dz, bordj-bou-arreridj.mta.gov.dz, biskra.mta.gov.dz, constantine.mta.gov.dz, djelfa.mta.gov.dz, djanet.mta.gov.dz, el-meniaa.mta.gov.dz, el-tarf.mta.gov.dz, ghardaia.mta.gov.dz, in-guezzam.mta.gov.dz, in-salah.mta.gov.dz, khenchela.mta.gov.dz, ouled-djellal.mta.gov.dz, medea.mta.gov.dz, oum-el-bouaghi.mta.gov.dz, relizane.mta.gov.dz, setif.mta.gov.dz, sidi-bel-abbes.mta.gov.dz, timimoun.mta.gov.dz, tizi-ouzou.mta.gov.dz, skikda.mta.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 de type XSS (Cross-Site Scripting)

2 - Mesures de sécurité préventives :
- Application d'un Web Application Firewall (WAF)
- Utilisation de balises HTML sanitaires pour limiter les risques XSS

Adresse IP : 197.112.0.130

Domaine(s) associé(s) : mail.mta.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	caldav	N/A	False	—	**Basse**
443	https	CommuniGate SPEC/8.0.8	False	—	**Basse**

Recommandations

1 - Risques potentiels :
- Exposition possible de services non-standard sur le port 443

2 - Mesures de sécurité préventives :
- Vérifier les services qui sont exposés sur le port 443
- Si nécessaire, configurer le firewall pour bloquer les services non-standard sur ce port

Adresse IP : 197.112.0.40

Domaine(s) associé(s) : portail.mta.gov.dz

Services détectés : 2

Port	Technologie	Version	Vulnérable	CVE	Criticité
80	http	nginx	False	—	**Basse**
443	ssl/http	nginx	False	—	**Basse**

Recommandations

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

2 - Mesures de sécurité préventives :
- Configurer un pare-feu pour bloquer les accès non autorisés
- Configurer les services web avec des règles de sécurité appropriées (authentification, autorisation, etc.)
- Utiliser des outils de scanning pour détecter des vulnérabilités et des failles
- Mettre en place des solutions de protection contre les attaques DDoS
- Utiliser des certificats SSL valides pour protéger les communications entre le serveur et les clients

- Mettre en place des solutions de détection et de réponse à l'intrusion pour détecter et répondre aux attaques
- Mettre en place des solutions de journalisation pour enregistrer les événements de sécurité et les analyses pour détecter des anomalies
- Mettre en place des solutions de gestion des mots de passe pour protéger les comptes administrateurs
- Mettre en place des solutions de protection contre les attaques par injection SQL
- Mettre en place des solutions de protection contre les attaques par XSS
- Mettre en place des solutions de protection contre les attaques par injection de code
- Mettre en place des solutions de protection contre les attaques de phishing
- Mettre en place des solutions de protection contre les attaques de spam
- Mettre en place des solutions de protection contre les attaques de spam bot
- Mettre en place des solutions de protection contre les attaques de spam de m