■ SDV Toolbox - Rapport de Sécurité

Outil:	SSLyze
Date:	07/06/2025 à 17:50:36
Cible:	isrp.fr:443
Opérateur:	SDV Security Team

■ Rapport d'Analyse SSL/TLS SSLyze

■ PROBLÈMES CRITIQUES SSL/TLS DÉTECTÉS

Métrique	Valeur
■ Domaine analysé	isrp.fr
■ SSL/TLS configuré	Oui
■ Problèmes critiques	4
■■ Avertissements	2
■ Certificat valide	Non
■■ Protocoles supportés	0
■ Date d'analyse	07/06/2025 à 17:50:36

■ Informations du certificat :

Propriété	Valeur
Émetteur	R11
Numéro de série	457591635383401104520140253938448836094421

■ Vulnérabilités SSL/TLS détectées :

Vulnérabilité	Gravité	Description
ROBOT Attack	ÉLEVÉ	Vulnérabilité dans l'implémentation RSA
Heartbleed	CRITIQUE	Fuite de mémoire OpenSSL

■ Extrait du rapport technique :

```
CHECKING CONNECTIVITY TO SERVER(S)
----------------------------------

isrp.fr:443 => 95.128.40.112


SCAN RESULTS FOR ISRP.FR:443 - 95.128.40.112
--------------------------------------------

* Certificates Information:
Hostname sent for SNI: isrp.fr
Number of certificates detected: 1
```

```
Certificate #0 ( RSAPublicKey )
SHA1 Fingerprint: 755a23df5ecc60f30d49d50ff87faae6ec7c7b46
Common Name: isrp.fr
Issuer: R11
Serial Number: 457591635383401104520140253938448836094421
Not Before: 2025-05-26
Not After: 2025-08-24
Public Key Algorithm: RSAPublicKey
Signature Algorithm: sha256
Key Size: 4096
Exponent: 65537
SubjAltName - DNS Names: ['isrp.fr', 'marseille.isrp.fr', 'vichy.isrp.fr', 'www.isrp.fr']

Certificate #0 - Trust
Android CA Store (14.0.0_r9): OK - Certificate is trusted
```

■■ Recommandations de sécurité SSL/TLS :

- ■ URGENT : Corrigez les vulnérabilités SSL/TLS critiques détectées
- Mettez à jour immédiatement votre configuration SSL/TLS
- Désactivez les protocoles et chiffrements obsolètes
- ■ Installez un certificat SSL/TLS valide et vérifié
- ■ Activez TLS 1.3 pour une sécurité optimale
- ■■ Configurez des suites de chiffrement sécurisées uniquement
- ■ Effectuez des tests SSL/TLS réguliers avec SSLyze
- ■ Mettez à jour régulièrement vos certificats SSL/TLS
- ■ Formez les équipes aux bonnes pratiques SSL/TLS
- ■ Implémentez HSTS (HTTP Strict Transport Security)
- ■ Surveillez l'expiration des certificats
- ■ Utilisez des certificats avec des algorithmes SHA-256 ou supérieurs