# Sécurité et Durcissement des Applications Node.js en Environnement de Production

*Lien : https://innov-systems.com/formation/securite-et-durcissement-des-applications-nodejs-en-environnement-de-production*

DURÉE
**3 jours (21h)**

RÉFÉRENCE
**SEC312**

CATÉGORIE
**Sécurité des Systèmes et Serveurs**

Innov Systems

## OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Identifier les vulnérabilités spécifiques aux environnements Node.js et leurs impacts potentiels
- Mettre en œuvre les meilleures pratiques de développement sécurisé adaptées aux projets Node.js
- Intégrer des mécanismes de durcissement, d’audit et de supervision continue dans le cycle de vie applicatif
- Renforcer la sécurité des API, des flux de données et des dépendances
- Savoir auditer et corriger une application Node.js déployée en production

## POUR QUI ?

- Développeurs backend Node.js
- Architectes techniques et chefs de projet web
- Administrateurs système responsables du déploiement et de la maintenance d’applications Node.js en production

## Programme détaillé

### 1 / INTRODUCTION À LA SÉCURITÉ DES APPLICATIONS NODE.JS

- Enjeux de la cybersécurité dans les environnements Node.js
- Typologie des menaces : du code malveillant aux attaques réseau
- Erreurs fréquentes dans les projets Node.js et leurs conséquences

### 2 / ARCHITECTURE NODE.JS ET SURFACE D'ATTAQUE

- Comprendre le modèle asynchrone et ses implications sécuritaires
- Risques liés au non-blocking I/O et à la gestion concurrente
- Gestion des dépendances et vulnérabilités via npm

### 3 / FONDAMENTAUX DES VULNÉRABILITÉS WEB

- Comprendre les principes d'authentification et d'autorisation
- Présentation du référentiel OWASP Top 10 et de ses impacts pour Node.js
- Introduction à la politique de sécurité des en-têtes HTTP

### 4 / MISE EN PRATIQUE : IDENTIFICATION DES FAILLES DE BASE

- Analyse d'une mini-application volontairement vulnérable
- Détection de vulnérabilités XSS et injections simples
- Discussion collective sur les correctifs à apporter

### 5 / CONTRER LES INJECTIONS ET LES FAIBLESSES D'ENTRÉE

- Prévention des injections SQL et NoSQL
- Validation robuste des entrées avec Joi, Yup ou Zod
- Protection contre les injections de commandes et la désérialisation non sécurisée

Innov Systems

## 6 / GESTION SÉCURISÉE DE L'AUTHENTIFICATION ET DES SESSIONS

- Sécurisation des JWT, cookies et tokens d'accès
- Implémentation de stratégies de rotation et d'expiration
- Stockage sécurisé des secrets et des credentials (dotenv, Vault, etc.)

## 7 / CHIFFREMENT ET PROTECTION DES DONNÉES

- Utilisation des modules de chiffrement natifs (crypto, bcrypt, Argon2)
- Gestion des certificats SSL/TLS et sécurisation des connexions HTTPS
- Sécurisation des données en transit et au repos

## 8 / SÉCURISATION DES API ET DES ÉCHANGES CLIENT-SERVEUR

- Bonnes pratiques REST et GraphQL
- Protection contre le brute-force : rate limiting et IP filtering
- Application de politiques CORS et CSP
- Gestion fine des droits d'accès avec RBAC/ABAC

## 9 / MISE EN PRATIQUE : RENFORCEMENT D'UNE API NODE.JS

- Implémentation d'une API REST sécurisée avec JWT et validation des entrées
- Mise en place de rate limiting et journalisation des accès
- Tests de sécurité unitaires avec Mocha et Chai

## 10 / AUDIT ET SURVEILLANCE DES DÉPENDANCES

- Analyse et correction des vulnérabilités avec npm audit, Snyk et OWASP Dependency-Check
- Mise en place de contrôles automatisés dans la chaîne CI/CD
- Gestion proactive des mises à jour de packages

## 11 / JOURNALISATION ET SUPERVISION SÉCURISÉE

- Bonnes pratiques de logs (éviter la fuite d'informations sensibles)

Inov Systems

- Centralisation et monitoring via Winston, ELK, ou Grafana Loki
- Détection d’incidents et alertes en temps réel

### 12 / AUDIT DE SÉCURITÉ D’APPLICATIONS NODE.JS

- Techniques d’audit statique et dynamique du code source
- Utilisation de scanners open source : OWASP ZAP, Burp Suite Community
- Analyse de configuration et de permissions

### 13 / DURCISSEMENT DE L’ENVIRONNEMENT DE DÉPLOIEMENT

- Sécurisation du serveur Node.js (headers, CORS, middleware Helmet)
- Protection des environnements Docker et CI/CD
- Bonnes pratiques de déploiement sécurisé (reverse proxy, WAF, MFA)

### 14 / MISE EN PRATIQUE : AUDIT ET RENFORCEMENT D’UNE APPLICATION EN PRODUCTION

## Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Innov Systems

## Prochaines dates programmées

| | |
|---|---|
| 09 au 11 Déc. 2026 | Distanciel |
| 17 au 19 Fév. 2027 | Présentiel - Casablanca |
| 14 au 16 Avr. 2027 | Présentiel - Casablanca |
| 09 au 11 Juin 2027 | Présentiel - Casablanca |
| 11 au 13 Août 2027 | Présentiel - Casablanca |

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

## Réservation & Renseignements

**Téléphone :** +212 522 247 210
**Email :** contact@innov-systems.com
**Web :** https//www.innov-systems.com


Innov Systems — Tous droits réservés

Innov Systems