# AVIS DE SECURITE

| | |
|---|---|
| **Objet** | **Multiples vulnérabilités dans les produits Elastic (Elasticsearch, Kibana, Logstash, Elastic Agent)** |
| **Niveau de criticité** | **IMPORTANT** |
| **Référence** | SNCSIRT-2026-ADS-301 |
| **TLP** | WHITE |

**Résumé**

Elastic a publié le 03/11/2026 une série de bulletins de sécurité (ESA-2026-200 à ESA-2026-238) corrigeant de multiples vulnérabilités dans la suite Elastic Stack. Les plus sévères sont CVE-2026-111497 (CVSS v3.1 : 8.1, écriture hors limites du décodeur Brotli de Node.js dans Elastic Agent), CVE-2026-115290 (CVSS v3.1 : 7.5, déni de service à distance d'Elasticsearch) ainsi que CVE-2026-91403, CVE-2026-114820 et CVE-2026-114406 (CVSS v3.1 : 7.4, racines de certification eMudhra non fiables dans Logstash et Kibana).

**Risque de sécurité**

- Exécution de code arbitraire à distance
- Déni de service à distance
- Atteinte à la confidentialité des données (interception TLS, divulgation d'informations)
- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité (autorisations)

**Systèmes affectés**

- Elasticsearch, Kibana, Logstash, Elastic Agent, APM Server, Heartbeat, Packetbeat, Elastic Maps Server et images Docker Elastic
- Versions 8.x antérieures à 8.19.24
- Versions 9.0.0 à 9.4.8 (antérieures à 9.4.9)
- Versions 9.5.0 à 9.5.5 (antérieures à 9.5.6)

**Recommandations**

1. Mettre à jour les produits Elastic vers les versions 8.19.24, 9.4.9 ou 9.5.6 (ou ultérieures) ;
2. Se référer aux bulletins de sécurité de l'éditeur du 03/11/2026 :
   - https://discuss.elastic.co/t/elastic-agent-8-19-24-9-4-9-9-5-6-security-update-esa-2026-234/391371
   - https://discuss.elastic.co/t/elasticsearch-8-19-24-9-4-9-9-5-6-security-update-esa-2026-201/391356
   - https://discuss.elastic.co/t/logstash-8-19-24-9-4-9-9-5-6-security-update-esa-2026-228/391365
   - https://discuss.elastic.co/t/kibana-8-19-24-9-4-9-9-5-6-security-update-esa-2026-229/391366

**Adresse :** Avenue Leopold S. Senghor, BP: 4026, Dakar
https://www.stcc-ssi.sn/

**E-mail :** sncsirt@dcssi.sn

**Date de publication : 06/11/2026**