



CENTRE D'EXPERTISE ET DE DONNÉES SUR LA NATURE

---

Paris, le 1 octobre 2025

**Objet** : Point d'information sur les services numériques portés par PatriNat dans le cadre de la cyberattaque du Muséum

Madame, Monsieur,  
Cher.chère collègue, partenaire ou participant

Comme vous le savez, **le Muséum national d'Histoire naturelle subit une attaque informatique sévère** entraînant la mise à l'arrêt d'une grande partie des systèmes, sites web et des outils mis en œuvre par PatriNat (OFB, MNHN). Le présent courrier a pour but de vous donner une vision d'ensemble de la situation et de vous tenir informé.e des perspectives.

#### **Rappel de la situation**

Le 28 juillet 2025, l'ensemble des systèmes informatiques du Muséum a été victime d'une cyberattaque visant au cryptage des données scientifiques et administratives portées par l'établissement, dont celles liées à l'inventaire du patrimoine naturel (INPN, TaxRef, HabRef, base des espaces protégés, Znieff, INPG, CardObs/CarHab, INPN Espèces, DEPOBIO, GINCo, FSD, BOB, SPOT, etc.).

Cette attaque s'est poursuivie pendant les mois d'août et de septembre, et le niveau de risque reste encore à ce jour très élevé.

Les sauvegardes mises en place par le Muséum sur bandes physiques sont *a priori* intègres mais toutes les bases n'ont pas encore pu être vérifiées. Le risque de perte de données porte en particulier sur celles saisies quelques semaines en amont de l'attaque.

#### **Premières actions engagées depuis la cyberattaque**

Les partenaires de PatriNat et les usagers de ses services ont rapidement été informés de la situation via les listes mails disponibles, avec notamment un enjeu de sécuriser les mots de passe. Plus de 90 000 usagers ayant un compte sur l'INPN ont ainsi été contactés.

Pour assurer une continuité de service dans ce contexte d'urgence, une page temporaire a été créée début août sur le site de l'unité PatriNat : <https://www.patrinat.fr/fr/actualites/une-page-temporaire-pour-telecharger-les-referentiels-de-donnees-lies-linpn-7354>

Elle permet de télécharger certains référentiels de données (par exemple TaxRef, la base de données Znieff, la couche des aires protégées, les fiches PDF Znieff et Natura 2000, etc.) et propose les liens vers les plateformes régionales du SINP et vers le site du GBIF pour l'accès aux données d'observation d'espèces. Cette page est mise à jour et complétée au fur et à mesure des demandes et de notre capacité à y donner suite.

Ces éléments sont régulièrement relayés sur les réseaux sociaux, notamment sur LinkedIn ([INPN](#) et [PatriNat](#)). Par ailleurs, nous avons mis en place une cellule de crise interne chargée de recenser et de répondre dans la mesure du possible aux demandes de données à partir des sauvegardes disponibles à notre niveau.

### Contexte actuel

L'expertise informatique a montré que les systèmes utilisés n'offraient pas toujours les conditions de sécurité satisfaisantes. Aussi, pour relancer nos outils en limitant les risques de nouvelle attaque, il nous faut les remonter sur une nouvelle infrastructure plus robuste.

Une fois cette nouvelle infrastructure en place, le Muséum pourra engager la réinstallation des applications administratives – priorité 1 (cible novembre 2025), puis celle des applications métiers et scientifiques (fin 2025 et 2026).

Les systèmes d'informations liés à l'expertise portés par PatriNat pour le compte du ministère de la Transition écologique, de l'OFB et du Muséum sont bien identifiés dans le plan d'action global de reconstruction des systèmes. Les outils réglementaires (DEPOBIO) puis ceux en « *cœur de mission* » (INPN, NatureFrance, Taxref, entrepôt indicateurs, FSD Natura 2000, BOB-SPOT) font partie des priorités.

### Perspectives de reconstruction

La remise en marche des différents services informatiques nécessite deux éléments :

- une infrastructure sécurisée pour redéployer les applications,
- l'accès aux sauvegardes physiques de données pour les exploiter et les remettre à disposition dans les outils numériques.

Le passage sur une infrastructure externe, plus performante et plus sécurisée impose de faire monter en version de nombreuses briques logicielles. Cette évolution constitue plus qu'un simple redéploiement et présente l'avantage d'accélérer les refontes déjà engagées avant la cyberattaque, dans le cadre du plan de modernisation porté par le Muséum et dans la stratégie de PatriNat de refonte de certains outils pour simplifier et améliorer la performance des services.

Depuis la semaine du 22 septembre, nos équipes techniques disposent d'un premier niveau d'accès à un nouvel environnement qui va permettre de démarrer les travaux de réinstallation. De plus, la priorisation de l'accès aux sauvegardes a été établie avec le service informatique du Muséum.

Un plan d'action opérationnel est en cours d'élaboration. Il doit prendre en compte les priorités stratégiques, la gestion des dépendances entre les outils et données, et les moyens techniques mobilisables. Il est important de noter que, **pour la majorité des programmes/sites/outils, la remise en service se fera très certainement en 2026**. Pour certaines applications, trop anciennes, une refonte sera nécessaire, ce qui impliquera un délai important de redéploiement.

Nous avons tout à fait conscience de l'impact de la situation pour vos activités. Notre objectif est de trouver le bon compromis pour restaurer les services numériques essentiels dans les meilleurs délais, tout en nous projetant sur des systèmes d'information sécurisés, performants et durables.

Nous vous remercions pour les nombreux messages de soutien reçus ces dernières semaines et pour votre compréhension pendant cette période compliquée. Dans ce contexte sans précédent, toutes nos équipes sont mobilisées afin de rétablir l'accès aux outils dans les meilleurs délais. Nous vous informerons régulièrement des avancées.

Très cordialement,

Laurent PONCET et Julien TOUROULT  
Directeurs de PatriNat

