

L'ANSSI publie le rapport d'incident sur les cyberattaques ayant touché la DGFIP

Publié le mardi 29 septembre 2026

Le Premier ministre a demandé à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) un audit approfondi de la Direction générale des finances publiques (DGFIP), à la suite des cyberattaques qui l'ont touchée cet été.

L'ANSSI a ainsi conduit un travail d'investigation afin de retracer la chronologie des activités illégitimes ayant été observées sur les systèmes d'information de la DGFIP entre mai 2026 et août 2026, ainsi que d'identification de mesures qui auraient pu permettre la détection et/ou la prévention de ces actes. Remis au Premier ministre le jeudi 24 septembre 2026, ce rapport est publié ce jour.

Les investigations ont permis de retracer les événements menant à des exfiltrations de données sur deux périmètres : le premier revendiqué le 12 août, concernant la plateforme impots.gouv.fr et le second revendiqué le lendemain, concernant des données cadastrales détenues par la DGFIP.

Le rapport met en évidence que la compromission des systèmes d'information de la DGFIP est la conséquence de l'exploitation de faiblesses dans trois domaines :

- **La gestion des identités** : les attaquants ont été en mesure de voler et d'utiliser des identifiants de connexion légitimes d'utilisateurs de la DGFIP. La récupération illégitime de ces identifiants est consécutive à leur utilisation sur des équipements personnels couplée à l'absence d'authentification forte sur les portails donnant accès à des ressources sensibles.
- **L'architecture** : des applications sensibles sont exposées, pour répondre à un besoin métier, sur Internet ou accessibles depuis le Réseau interministériel de l'État (RIE) sans cloisonnement, augmentant leur exposition et ouvrant un risque de latéralisation depuis des ressources d'organismes tiers (comme cela a été le cas depuis le ministère de l'Éducation nationale).
- **La détection** : Aucune de ces deux vagues d'exfiltration n'a été détectée, ni par les moyens de supervision de la DGFIP ni par ceux de l'ANSSI, révélant les lacunes dans la supervision des systèmes d'information de la DGFIP. Du côté de la DGFIP, les solutions de détection au niveau applicatif n'ont pas été en mesure d'identifier les accès suspects. En effet, ses équipes ne supervisaient jusqu'ici pas l'un des portails utilisés par l'attaquant pour exfiltrer des informations et aucun mécanisme n'a corrélé les signaux suspects. Du fait du placement de ses sondes de détection, de l'absence de marqueurs de compromission réseau pertinents et de règles de détection spécifiques à cette menace, l'ANSSI n'a pas été en mesure de détecter les comportements suspects.

Un plan d'action prenant en compte les défaillances exploitées a été défini avec la DGFIP, le rapport identifiant également des améliorations à apporter aux capacités de détection et à la coordination interministérielle.

2 d'articles

PC

Partager cette page



