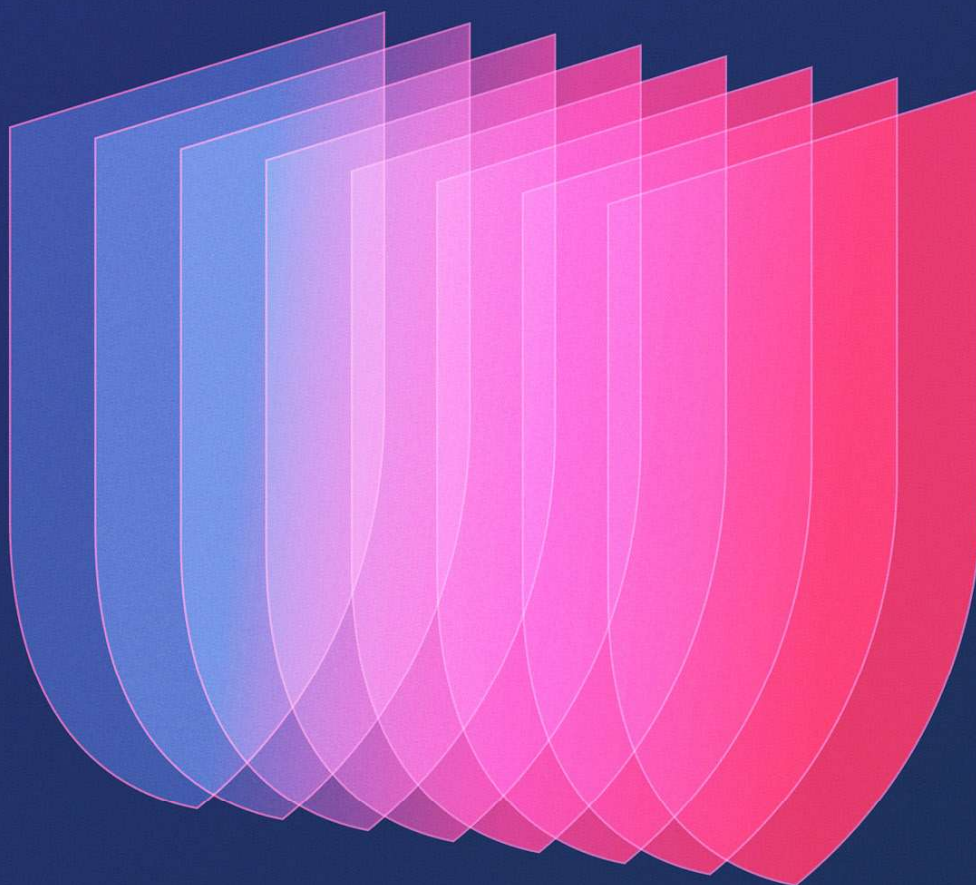


REACTIV

Point de situation Septembre 2026



PRESENTATION DE L'OPERATION

Face à l'intensification des attaques cybercriminelles liées à des violations de données affectant les services de l'Etat, le Premier ministre a demandé le 1^{er} septembre 2026 à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de mettre en place une capacité renforcée de réaction, d'intervention et d'assistance aux services de l'État.

Baptisé « **REponse & ACTION Interministérielle face aux Violations de données** » (**REACTIV**), ce dispositif opérationnel permet de mobiliser immédiatement les compétences et les moyens nécessaires à l'Agence aux côtés des ministères concernés.

L'opération de cyberdéfense REACTIV consiste ainsi en un basculement immédiat des efforts opérationnels de l'ANSSI pour renforcer l'appui qu'elle fournit aux ministères dans le traitement des compromissions de comptes utilisateurs et dans l'analyse des violations de données.

Ce renforcement doit permettre de mieux circonscrire les attaques et de lutter plus réactivement contre les exfiltrations de données. Il complète les mesures de la [Feuille de route des efforts prioritaires en matière de sécurité numérique de l'Etat 2026-2027](#), dont le Premier ministre a demandé l'accélération de la mise en œuvre, afin de réhausser significativement et durablement le niveau de sécurité des réseaux ministériels.

Dans le cadre de cette opération, l'autorité de l'ANSSI est renforcée avec :

- La possibilité pour l'Agence de faire prendre aux ministères, dans des délais contraints, les mesures d'urgence qui s'imposent pour protéger les données des citoyens confiées aux administrations ;
- La mise en place d'une communication technique de crise centralisée par l'ANSSI en cas d'attaque relative à cette menace touchant des services de l'État.

Le présent document est un point de situation qui reflète des travaux d'investigation en cours et des incidents qui évoluent rapidement. De fait, les éléments et données chiffrées associées sont susceptibles d'évoluer et ne peuvent constituer une vision parfaitement exhaustive, à une date donnée, de la situation opérationnelle relative aux violations de données affectant l'Etat.

Tendance globale

Depuis le 1^{er} août 2026, 99 violations de données ont été portées à la connaissance de l'ANSSI. Sur l'ensemble de ces événements de sécurité¹, 67 sont confirmés dont 32 en cours de traitement par l'ANSSI.

Vulnérabilités récurrentes

- **Vulnérabilité Metabase (CVE-2026-72898)** : une exploitation massive de la vulnérabilité est observée depuis début août 2026. Cette vulnérabilité, de type injection SQL, permet l'accès à la base de données de l'application Metabase pour un utilisateur non authentifié et l'obtention des droits administrateurs de l'instance. Neuf instances au sein de ministères ont ainsi été compromises. Le correctif est disponible depuis le 6 août 2026. L'ANSSI a demandé à l'ensemble des ministères d'identifier leurs instances et de vérifier leur mise à jour. [Voir le bulletin d'alerte du CERT-FR](#).
- **Compromission de comptes par le biais d'infostealers²** : les identifiants³ volés sur des postes personnels utilisés dans un cadre professionnel, ou issus de précédentes violations de données, permettent l'accès à des services exposés sans double authentification et restent un vecteur initial marquant sur cette période.
- **Vulnérabilités de type IDOR⁴** : l'ANSSI a recensé plusieurs exploitations de ce type de vulnérabilités dans le périmètre ministériel. Ainsi, parfois combinées à d'autres faiblesses, elles ont rendu possible l'exfiltration massive de documents.
- **Absence de double authentification (MFA) ou authentification faible** : facteur clé de nombreux incidents analysés par l'ANSSI, l'absence de MFA, ou l'utilisation d'un second facteur faible (e-mail), a facilité les intrusions puisqu'un mot de passe faible ou une fuite de mot de passe suffisait à l'attaquant pour s'octroyer *a minima* un accès utilisateur.
- **Sous-traitance et chaîne d'approvisionnement** : un incident illustre le risque de compromission par rebond. La compromission du prestataire a eu pour conséquence le vol dans les infrastructures du prestataire de certaines données concernant le ministère.
- **Défauts de développement et de configuration** : plus marginalement utilisées comme vecteur d'intrusion dans les incidents recensés, mais présentes couramment dans les incidents portés à la connaissance de l'ANSSI, des faiblesses et vulnérabilités courantes

¹ Un événement de sécurité comprend des signalements et incidents. Les signalements correspondent à des événements indésirables ou inattendus menaçant la sécurité d'un système d'information. Il s'agit d'un incident lorsque ces événements relèvent d'une compromission avérée ou d'une attaque réussie.

² Un *infostealer* est un programme destiné à voler des informations sensibles par exemple des données de connexion.

³ Terme qui désigne l'interprétation imprévue d'un code SQL, introduit par une voie détournée, dans une application.

⁴ Une vulnérabilité de type IDOR (Indirect Object Reference) permet d'accéder à un objet sans authentification ou identification préalable. Les vulnérabilités de type traversée de répertoire en font partie.

telles que l'absence de contrôle des autorisations, des injections SQL, ou des fichiers exposés peuvent conduire à des violations de données.

Impacts principaux

Les incidents ont exposé des catégories de données variées, touchant tant des agents de l'État que des usagers et des professionnels, et notamment :

- **Données fiscales et patrimoniales** : près de 353 000 usagers particuliers (revenu fiscal de référence, taux de prélèvement à la source, identité, coordonnées), 252 000 usagers professionnels (raison sociale, SIREN, coordonnées) et 434 000 propriétaires dans le cadre du serveur cadastral.
- **Données d'identification et de contact** : plus de 30 000 utilisateurs de l'Agence pour l'enseignement français à l'étranger, 275 000 utilisateurs du Service national universel, 3 millions de numéros de téléphone pour Bloctel, 5 265 personnes pour Préférence Formation.
- **Données professionnelles et administratives** : identifiants fiscaux, numéros SIREN/SIRET, données de certification, qualifications, expériences, données relatives aux enseignants, données de contrôleurs techniques.
- **Données techniques et d'exploitation** : journaux de connexion, métadonnées d'applications, identifiants de comptes techniques, mots de passe hachés.
- **Données de messagerie et conversations** : échanges sur Tchap ou par messagerie électronique, courriels de support.

Des communications aux personnes concernées ont été effectuées lorsque la nature des données le justifiait.

Travaux de l'ANSSI

L'ANSSI assure la coordination technique, le partage de marqueurs d'attaque ainsi qu'un appui à l'analyse forensique et à la remédiation. Elle a également piloté la diffusion d'alertes sur la vulnérabilité Metabase (CVE-2026-72898) et accompagné le durcissement des authentifications sur les portails exposés.

Ministère de l'Éducation nationale

Depuis juillet 2026, le ministère de l'Éducation nationale a rapporté différents incidents de sécurité visant plus d'une dizaine d'académies. Des latéralisations ont été mises en évidence et l'attaquant a pu avoir accès à plusieurs services nationaux déconcentrés et exfiltrer des données. Le ministère s'est rapidement mobilisé pour mettre en œuvre un plan de continuité d'activité et déployer des mesures de remédiation à un rythme soutenu afin de pouvoir ouvrir les services pour la rentrée.

GAIA : fin juillet 2026, le ministère de l'Éducation nationale a détecté une intrusion sur ses systèmes d'information et en a informé l'ANSSI. L'attaquant a potentiellement pu exfiltrer les données de 4,35 millions d'enseignants (identité, affectation, grade, formation, indemnités).

SIECLE : une revendication publique le 17 août 2026 fait état d'une exfiltration de données personnelles concernant des enseignants et élèves. Il s'agit pour partie d'une reprise des données de l'incident GAIA. Cette communication a aussi révélé l'exfiltration de la base élèves de SIECLE de l'académie de Créteil d'un million d'élèves, de leurs responsables légaux et d'enseignants.

Tchap : le 19 août, la DINUM détecte la compromission d'un compte Tchap d'un agent de l'Education nationale. Le compte a été utilisé pour accéder à des salons publics et privés auquel le compte compromis avait déjà accès, dont certains de la DGFIP et du cadastre. Les conversations accessibles au compte ont été exfiltrées. Le compte a été sécurisé (réinitialisation mot de passe, révocation des sessions, blocage du compte externe).

Service national universel (SNU) : le 7 septembre, l'ANSSI est informée de la revendication d'une fuite de données sur un portail du SNU via l'exploitation d'une faille IDOR. Cela aurait exposé 275 000 utilisateurs (identifiants, noms, courriels, téléphones, rôles, statuts, informations géographiques, activité). Les investigations sont en cours.

Ministère de l'Europe et des Affaires étrangères

Le 12 août 2026, l'Agence pour l'enseignement français à l'étranger (AEFE) a été la cible d'une violation de données. Un compte compromis a permis d'accéder à l'annuaire interne et d'extraire des informations sur plus de 30 000 personnes. Les données concernées portent sur l'identité, les coordonnées, les certifications professionnelles, les qualifications, les expériences, les évaluations et le financement des parcours de validation des acquis de l'expérience.

Ministères Économiques et Financiers

Bloctel : le 7 août 2026, le service d'opposition au démarchage téléphonique a subi une violation de données. Les données ont été exfiltrées depuis un compte professionnel d'une entreprise : l'attaquant a téléchargé une archive contenant la liste des numéros soumis par le professionnel ainsi que la liste des numéros après traitement par Bloctel, permettant d'identifier par différence environ 600 000 numéros inscrits sur Bloctel. Le service a été définitivement fermé le 11 août 2026.

TRACFIN : une compromission a touché le sous-traitant de l'opérateur du module d'assistance aux usagers du portail de télédéclaration utilisé par les professionnels assujettis afin de transmettre leurs déclarations à TRACFIN. Cette compromission a conduit à une exfiltration de données entre fin juin et mi-juillet 2026. 136 assujettis sont concernés (nom, prénom, fonction, courriel, téléphone) ainsi que le contenu de 213 demandes d'assistance envoyées par ces utilisateurs au support technique. Aucune donnée sensible relative aux déclarations de soupçon n'a été exposée. L'administration visée a cessé toute relation avec ce prestataire. Les investigations se poursuivent pour identifier de potentielles autres victimes indirectes de la compromission du sous-traitant.

Direction générale des douanes et droits indirects (DGDDI) : le 21 août 2026, à la suite des partages de marqueurs techniques par l'ANSSI, le CSIRT de la DGDDI a établi le lien entre la compromission de trois comptes de messagerie d'agents, avec exfiltration de données, et celle d'un serveur utilisé pour les échanges entre agents et prestataires auquel avait accès un des comptes. Des mesures de renforcement ont été rapidement mises en œuvre sur la messagerie, notamment des travaux de remplacement du dispositif d'authentification, le retrait de l'accès mail depuis internet, ainsi que la coupure définitive de la solution de partage via le serveur d'échange.

Direction générale des finances publiques (DGFIP) : plusieurs incidents – détectés les 12 et 13 août 2026 et traités conjointement – ont touché la DGFIP. Le premier concerne une exfiltration de données fiscales concernant environ 353 000 usagers particuliers (état civil, coordonnées, identifiant fiscal, situation familiale, revenu fiscal de référence, taux de prélèvement à la source, liste demandes) et 252 000 professionnels (SIREN, dénomination, adresse, liste de demandes). Le deuxième incident vise le serveur professionnel de données cadastrales. Un compte compromis de géomètre-expert d'un cabinet privé a permis l'exfiltration d'environ 2 millions de données cadastrales concernant environ 434 000 usagers (noms, dates de naissance, adresses, identifiants fonciers, parcelles, nature des droits). Des tentatives d'accès ont aussi été identifiées au Portail internet de la gestion publique (PIGP) à l'aide d'identifiants compromis par le biais d'*infostealers* sur des postes personnels ou de partenaires. Dans le cadre de ces incidents, l'ANSSI conduit une revue des investigations et du plan de remédiation de la DGFIP. Un plan d'audit est également mis en œuvre, accompagné par l'ANSSI qui pilote, avec la DGFIP, le lancement d'un premier audit réalisé par un prestataire d'audit de sécurité des systèmes d'information (PASSI).

Ministères de la Transition écologique, Aménagement du territoire, Transports, Ville et Logement

Plusieurs violations de données ont été identifiées par des entités rattachées au ministère de la Transition écologique, de la Biodiversité et des Négociations internationales sur le climat et la nature. L'ANSSI concentre ses efforts sur l'application Bureau numérique en conduisant une partie des investigations et un appui à la remédiation, tandis qu'un prestataire est en charge d'accompagner le ministère sur le traitement des incidents des autres directions. Un plan de remédiation est en cours de déploiement.

Bureau Numérique (BNUM) : le 25 août 2026, suite au partage de marqueurs de compromission par l'ANSSI, le ministère a détecté la compromission de plus de 300 comptes utilisateurs de l'application BNUM, permettant l'accès à une messagerie mutualisée entre ministères et à des espaces de travail. Le contenu des boîtes de messagerie et de l'espace de fichiers partagé a été exfiltré, des analyses sont en cours pour en identifier la teneur. Des levées de doute et recherches de vulnérabilités sont en cours sur de nombreux portails et applicatifs pour identifier d'autres latéralisations ou persistances. Les mots de passe compromis ont été renouvelés, la double authentification a été activée pour tous les utilisateurs de la messagerie et la vulnérabilité à l'origine de la compromission a été corrigée. Certains utilisateurs ne sont plus en mesure de se connecter à leurs comptes suite à l'activation de la double authentification.

OISO : une vulnérabilité sur le portail OISO (destiné à des contrôles techniques de respect de normes environnementales par des prestataires privés) du ministère a permis l'énumération de données personnelles de 22 000 agents et organismes agréés. L'attaquant a utilisé un compte compromis d'un organisme privé pour accéder aux données. Le portail a été mis hors ligne, isolé du réseau interministériel, la faille corrigée et les mots de passe réinitialisés.

Zéro Logement Vacant : le 28 août 2026, l'ANSSI est informée de la revendication de la compromission et du vol de données de la plateforme Zéro Logement Vacant, utilisée par les collectivités territoriales pour l'identification et le contact des propriétaires de logements durablement vacants afin de mettre en place des actions permettant la remobilisation du parc immobilier. Le point d'entrée serait la compromission d'une instance Metabase. De manière préventive, la base de données a été isolée et le service Zéro Logement Vacant coupé le temps des investigations. La violation concernerait 48 millions de propriétaires en France.

Signal Logement : un incident affecte l'application Signal Logement qui permet d'identifier les logements insalubres. L'incident est en cours de qualification.

Bureau des courriers parlementaires et réservés (BCPR) : un incident porte sur l'application BCPR dédiée aux communications entre la Direction générale de l'Aménagement, du Logement et de la Nature (DGALN) et les parlementaires. Des courriels auraient été exfiltrés. L'incident est en cours de qualification.

Qualicharge : l'exploitation d'une vulnérabilité Metabase a permis l'exfiltration de 102 000 sessions de recharge et d'une centaine de comptes techniques (identifiants, courriels, mots de passe chiffrés) depuis l'application dédiée à la gestion des infrastructures de recharge des véhicules électriques. La mise à jour a été appliquée, les sessions suspectes fermées.

Docurba : une exfiltration de données concernant les utilisateurs de la plateforme (collectivités territoriales, directions départementales des territoires, ministères) a été revendiquée le 25 août 2026. Il s'agit d'une application gérée par la DGALN rattachée au ministère. Les premiers travaux de qualification sur la revendication suggèrent une compromission datant de plusieurs mois. Les investigations afin d'identifier l'origine de la compromission se poursuivent mais les premiers éléments permettent d'envisager que l'attaquant a exploité une vulnérabilité sur une instance Metabase.

Services du Premier ministre

Laboratoire d'innovation de l'ANSSI : l'exploitation d'une vulnérabilité Metabase a entraîné la compromission de 118 comptes utilisateurs Metabase dont une trentaine de comptes d'utilisateurs externes (données statistiques d'utilisation, identifiants, courriels et mots de passe hachés). Des mesures de sécurisation ont été mises en place, notamment la mise à jour des instances vulnérables et un renouvellement des mots de passe pour l'ensemble des comptes. Les comptes n'ayant pas été utilisés depuis plus de trois mois ont été désactivés.

Direction interministérielle du numérique (DINUM) : deux instances Metabase (ProConnect et Nuage-Public) ont été compromises. Les données exfiltrées portent sur des informations administratives d'organismes publics (SIREN, SIRET, budgets, effectifs), des métadonnées de contributions à des projets logiciels open source, et des historiques de connexions anonymisés. Ces données sont déjà publiques. La DINUM a corrigé les vulnérabilités, réinitialisé les secrets, supprimé les comptes créés par l'attaquant.

Ministère du Travail et des Solidarités

France VAE : le portail a été compromis via la vulnérabilité Metabase le 8 août 2026. L'attaquant a obtenu un accès privilégié et exfiltré l'intégralité des données utilisateurs (identité, contact, certifications, qualifications, expériences, évaluations, financement). Une communication a été adressée aux utilisateurs concernés par l'incident. Des mesures de sécurisation ont été mises en place, notamment la mise à jour de l'instance vulnérable et un renouvellement des mots de passe pour l'ensemble des comptes.

Ministère de l'Agriculture, de l'Agro-alimentaire et de la Souveraineté alimentaire

Préférence Formation : la plateforme, dédiée à la formation professionnelle et gérée par le ministère de l'Agriculture, a fait l'objet d'une revendication d'exfiltration début septembre. La fuite porterait sur 5 265 personnes (identifiant, nom, prénom, courriel, ville, pays, fuseau horaire). Les investigations sont en cours.



REACTIV

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

51 boulevard de la Tour-Maubourg 75700 PARIS 07 SP

www.cyber.gouv.fr

