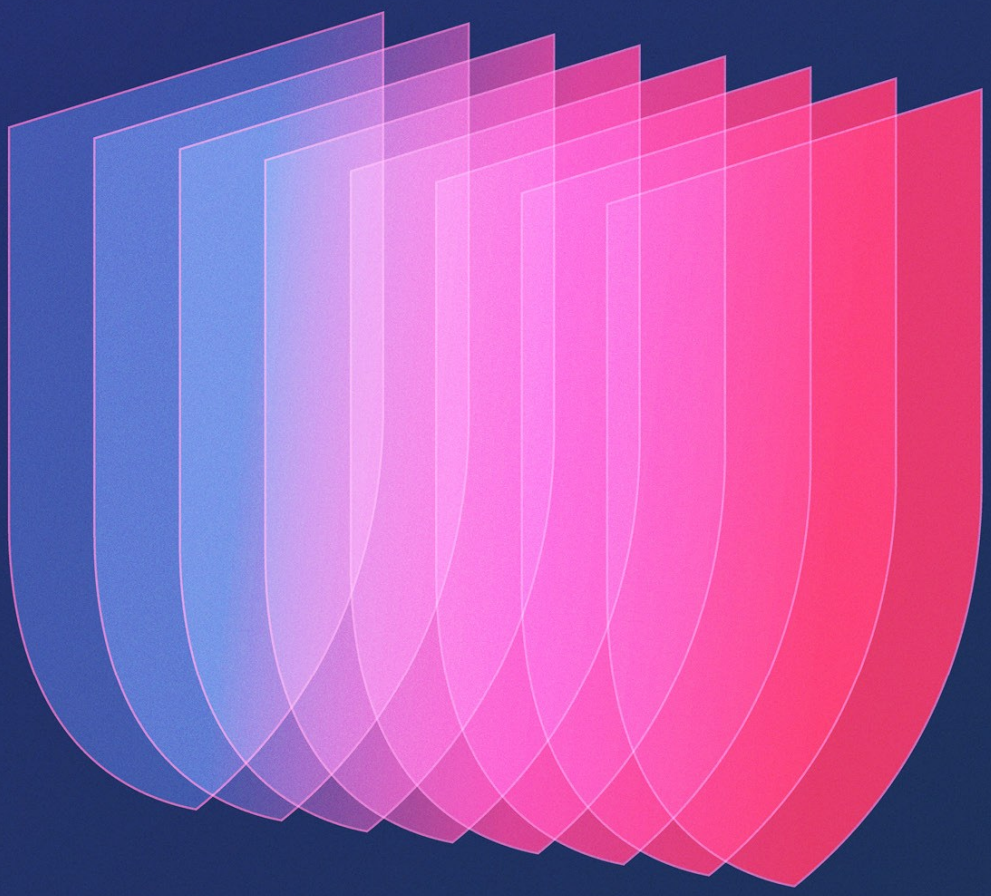
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

REACTIV

Point de situation
Octobre 2026



CERT-FR

1 RAPPEL SUR L'OPÉRATION

Face à l'intensification des attaques cybercriminelles liées à des violations de données affectant les services de l'État, le Premier ministre a demandé le 1er 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 pour intervenir 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 a d'ores et déjà permis de mieux circonscrire les attaques et de lutter contre les exfiltrations de données. Il contribue au déploiement opérationnel des mesures de la feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 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 systèmes d'information ministériels et interministériels.

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 le deuxième point de situation qui reflète des travaux d'investigation en cours et des incidents qui évoluent. 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'État.

Tendance globale

Depuis le 30 septembre 2026, date du dernier point de situation, 64 nouvelles violations de données ont été portées à la connaissance de l'ANSSI. Sur l'ensemble de ces événements de sécurité[1], 5 concernent des ministères ou des organismes sous tutelle et sont en cours de traitement par les victimes avec l'appui de l'ANSSI.[2]

Sur le périmètre des ministères, l'ANSSI souligne une baisse importante du nombre de violations de données détectées ou revendiquées depuis le dernier point de situation.

Vulnérabilités récurrentes

L'ensemble des violations de données exploitent des faiblesses et vulnérabilités déjà mentionnées dans le point de situation de septembre 2026[3]. Ces vulnérabilités font l'objet d'un traitement particulier par les ministères accompagnés par l'ANSSI :

- Absence de double authentification (MFA) ou authentification faible ;
- Sous-traitance et chaîne d'approvisionnement ;
- Compromission de comptes par le biais d'*infostealers*[4] ;
- Vulnérabilités de type *IDOR*[5] ;
- Défauts de développement et de configuration.

Les nouvelles violations de données n'ont pas souligné l'usage d'autres faiblesses ou vulnérabilités[6]. Si ces vulnérabilités restent d'actualité, il est à noter que les progrès sur les mesures de sécurisation sont significatifs, notamment sur la mise en œuvre du MFA. La réalisation d'ensemble des objectifs 2026 de la feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 2026-2027 progresse notablement et atteint 70% d'avancement au plan interministériel.

[1] Les événements de sécurité peuvent être des signalements ou des 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] Ces nouveaux incidents font l'objet de précisions dans la deuxième partie du document et comportent la mention [Nouveau].

[3] https://cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-006/

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

[5] Une vulnérabilité de type *IDOR (Indirect Object Reference)* permet d'accéder à un objet sans authentification, après une première authentification avec un compte qui n'est normalement pas autorisé à accéder aux données. Les vulnérabilités de type « traversée de répertoire » en font partie.

[6] Pour rappel, les vulnérabilités critiques qualifiées par l'ANSSI font l'objet de bulletins d'alerte publiés sur le site du CERT-FR : https://cert.ssi.gouv.fr

Impacts principaux

L'exfiltration de données personnelles demeure l'impact principal des violations de données observées en octobre :

- Données d'identité et d'authentification : Annuaires internes, condensats de mots de passe, comptes de service et de migration ;
- Données relatives aux mineurs : identités et dates de naissance d'enfants, réservations de séjours et dossiers d'aides ;
- Données sociales et financières : Dossiers d'allocataires (nom, matricule, quotient familial, composition familiale), informations de paiement et d'aides financières ;
- Données professionnelles et RH : Coordonnées d'agents (téléphones), données de gestion de formation des personnels sur plusieurs années ;
- Contenus de messagerie : Boîtes aux lettres accédées et exfiltrées pour tout compte compromis.

Des communications aux personnes concernées sont réalisées lorsque la nature des données le justifie.

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. L'ANSSI déploie notamment avec les ministères des plans de remédiation structurés. Ces plans s'appuient sur la feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 2026-2027 et sur sa déclinaison à travers des exigences techniques, socle minimal de sécurité pour se protéger de nouvelles compromissions, établies notamment à partir des investigations menées dans le cadre de REACTIV et des audits effectués.

Les analyses des signalements et les investigations menées dans le cadre des incidents convergent vers une technique récurrente : **la réutilisation de secrets volés pour accéder à des applications ministérielles** permettant aux attaquants d'extraire de manière légitime les données qu'elles hébergent.

Afin de s'en défendre, la première action d'endiguement consiste à renouveler les secrets d'authentification, compromis ou suspectés de l'être. Cette action doit s'accompagner d'une **protection renforcée des comptes** — mise en place systématique d'une **authentification forte**[7] et un contrôle strict des comptes à privilèges — ainsi que du **durcissement du filtrage des accès** pour empêcher l'exfiltration des données. Il est

[7] https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf

également impératif de **renforcer la sécurité des applications** notamment pour les services exposés à internet ou des réseaux tiers.

À ce titre, l'ANSSI a publié le 20 octobre un retour d'expérience[8] sur les violations de données applicatives.

Le travail mené sur l'opération REACTIV est étroitement coordonné avec les enquêtes judiciaires en cours par ailleurs. Elles constituent un volet essentiel de la réponse de l'État.

[8] https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-008.pdf

2 MISE À JOUR DES INCIDENTS

Ministère de l'Éducation nationale

De juillet à septembre 2026, le ministère de l'Éducation nationale a rapporté différents incidents de sécurité visant 25 des 30 académies avec des impacts opérationnels de criticité variable. 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. Un mode opératoire itératif des attaquants a été mis en évidence : obtention d'identifiants valides, exploitation de comptes à privilèges, recherche de nouveaux accès et exfiltration de données (annuaires, bases applicatives, boîtes aux lettres), voire latéralisation vers d'autres entités via le Réseau interministériel de l'État (RIE). Un plan de remédiation en plusieurs étapes a été construit avec l'ANSSI pendant l'été. Il est mis en œuvre à un rythme soutenu pour élever durablement le niveau de sécurité de l'ensemble des académies.
La remédiation engagée par plusieurs académies comme celles de Nantes ou de Toulouse a produit des résultats concrets : les comptes ont été réinitialisés et des services ont pu être réouverts progressivement depuis la rentrée en fonction des priorités de gestion. Les derniers chantiers menés avec l'accompagnement de l'ANSSI portent sur le durcissement des accès d'administration, une supervision renforcée des flux de données (limités aussi en nombre) ainsi que la sécurisation de certaines applications.
Aucune nouvelle violation de données n'a été constatée depuis la parution du rapport de septembre.

Ministère de l'Europe et des Affaires étrangères

[NOUVEAU] Portail des bibliothèques : une intrusion dans les environnements de production du portail des bibliothèques du MEAE a été détectée le 20 octobre 2026. Un tiers aurait accédé à des données personnelles d'une centaine d'utilisateurs (agents, bibliothécaires et usagers externes) en utilisant des comptes techniques volés en amont sur un serveur compromis. Les tentatives d'élévations de privilèges ont été bloquées. Les investigations se poursuivent avec le prestataire et le soutien de l'ANSSI.

Ministères économiques et financiers

Plusieurs incidents avaient touché la Direction générale des finances publiques (DGFIP) en août 2026 ayant entraîné l'exfiltration de données fiscales d'usagers particuliers et professionnels ainsi que de données cadastrales. Les investigations sont closes et font l'objet d'un rapport dédié[9]. La DGFIP conduit un plan de remédiation qui intègre les

[9] https://cyber.gouv.fr/actualites/lanssi-publie-le-rapport-dincident-sur-les-cyberattaques-ayant-touche-la-dgfip/

préconisations de REACTIV et plus largement de la feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 2026-2027. Plusieurs audits conduits par l'ANSSI sont en cours, qui vérifieront notamment l'effet de ce plan de remédiation

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

L'ANSSI concentre toujours ses efforts sur l'application Bureau numérique (BNUM) en poursuivant ses investigations et son appui à la remédiation. L'ANSSI a par ailleurs conduit un audit de recherches de vulnérabilités du code de l'application BNUM. Le plan de remédiation élaboré en septembre est en cours de mise en œuvre.

[NOUVEAU] Office français de la biodiversité (OFB) : le 4 octobre 2026, l'exploitation d'une vulnérabilité de type *IDOR* sur l'API de paiement du portail public d'inscription à l'examen du permis de chasser (permischasser.ofb.fr) a exposé les données personnelles de plus de mille personnes (dont des mineurs), publiées en accès libre le jour même. L'application a été mise hors ligne le soir, les usagers ont été informés individuellement avec un message de vigilance. Après correction des vulnérabilités, le site a pu être remis en ligne au cours du mois d'octobre.

Ministère du Travail et des Solidarités

[NOUVEAU] France Travail : le 8 octobre 2026, la vente de données de plus de 60 000 agents et professionnels (noms, e-mails professionnels, téléphones, fonctions, agences, identifiants internes) a été revendiquée sur un forum cybercriminel. La compromission, avec validation du second facteur (SMS), du compte d'un agent a permis l'exfiltration des données le 26 septembre. Le compte a été révoqué et les adresses IP malveillantes bloquées. Les investigations sont en cours avec l'appui de l'ANSSI.

[NOUVEAU] Caisse d'allocations familiales : Une violation de données concernant la plateforme vacaf.org du dispositif d'aide aux vacances (VACAF) des caisses d'allocations familiales a été détectée le 9 octobre 2026, à la suite d'une mise en vente de bases de données. La compromission d'identifiants de comptes de partenaires issus d'*infostealers* (sans double authentification) et l'exploitation d'une URL exposant les identifiants des dossiers (*IDOR*) ont permis une extraction automatisée de données entre le 8 et le 10 octobre. Près de 1,2 million de dossiers sont concernés (noms, matricules CAF, quotient familial, identités de mineurs, aides financières et réservations) ; aucune donnée bancaire ni mot de passe n'est concerné. Le service a été mis hors ligne. L'information des allocataires concernés est en cours et la remise en ligne, conditionnée à un test d'intrusion et à la mise en œuvre d'un mécanisme de double authentification, est prévue. Les investigations se poursuivent avec l'ANSSI.

Ministère de l'Agriculture, de l'Agroalimentaire et de la Souveraineté alimentaire

À la suite d'un partage de marqueurs, le ministère avait identifié des certificats VPN compromis. Néanmoins, l'authentification multifacteur a empêché l'attaquant de se connecter au VPN. Les investigations menées n'ont pas mis en évidence d'autre activité malveillante.

[NOUVEAU] Agence de service et de paiement : au cours des derniers mois, l'ASP[10], établissement public administratif chargé du versement de certaines aides, a fait l'objet de plusieurs violations de données sans lien identifié entre elles. En août, l'ASP a détecté que les portails PROFIL et PUMA avait été compromis permettant aux attaquants d'exfiltrer des données personnelles. Ces deux portails ont fait l'objet de correctifs et ont été réouverts.

Le 30 septembre 2026, le portail DEFI, permettant la rémunération des stagiaires, a été compromis via un compte usurpé et l'exploitation d'une vulnérabilité. L'attaque a été revendiquée le 9 octobre 2026 et le portail a immédiatement été isolé. L'exfiltration concerne 30 500 usagers qui ont été notifiés.

En lien avec ses ministères de tutelles et l'ANSSI, l'ASP a lancé un processus de durcissement de sa sécurité notamment par la revue et la sécurisation de ses différents portails et l'amélioration de la supervision et de la détection.

[10] Les Ministères de tutelles sont le Ministère de l'Agriculture et le Ministère du Travail et des Solidarités.

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