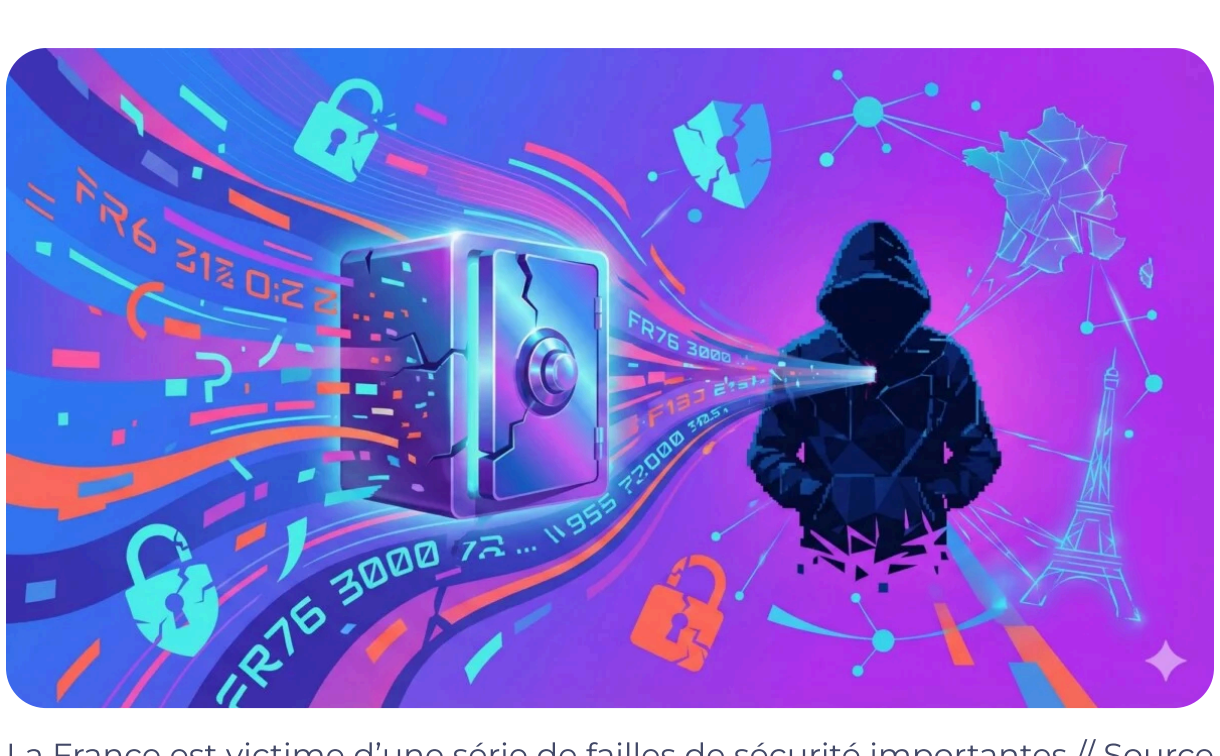
19 février 2026 · 15:49

PARTAGER



La France est victime d'une série de failles de sécurité importantes // Source : Généré par Frandroid avec Google Gemini

Vous ne le connaissez pas, mais lui, il vous connaît. IDMerit est un prestataire utilisé par les banques, en particulier les fintechs, pour faire de la vérification d'identité.

Une enquête de Cybernews a découvert une faille monstre : un outil IA d'IDMerit a laissé exposées les données concernant un milliard d'individus dans le monde. En France, ce sont près de 52 millions de comptes qui sont dans la nature.

Quelles sont les données volées ?

Contrairement à de vieilles fuites de données pêle-mêle, cette base est **parfaitement structurée**, ce qui en fait une véritable mine d'or pour les cybercriminels.

Voici les données qui ont été laissées accessibles :

- **Genre, noms et prénoms complets**
- **Adresses postales** (avec code postal)
- **Dates de naissance**
- **Cartes d'identité**
- **Numéros de téléphone**
- **Adresses e-mail**
- **Métadonnées d'opérateurs télécoms**

Il s'agit de données « *KYC* » (Know Your Customer), c'est-à-dire le genre de données que vous partagez avec votre banque pour prouver votre identité et réaliser des opérations sensibles sur vos comptes.

Autant d'informations précieuses qu'il sera possible pour un escroc de recouper avec les données issues de piratages comme celui de la DGCFIP.

Cette faille massive « *souligne à quel point les fournisseurs tiers d'identité sont devenus des infrastructures critiques et peuvent se transformer en points de défaillance catastrophiques.* »

Que s'est-il passé chez IDMerit ?

Le 11 novembre 2025, les chercheurs en cybersécurité de Cybernews ont donc découvert une base de données de près d'un téraoctet (1 To), hébergée sur une instance MongoDB. Cette **base de données était accessible à quiconque** s'y connectait. Pas de mot de passe, pas de pare-feu. Une porte grande ouverte sur le web.

Cette base appartiendrait à **IDMerit**, un prestataire qui aide les entreprises de la FinTech à vérifier l'identité de leurs clients en temps réel. Les chercheurs ont immédiatement alerté l'entreprise, qui a sécurisé l'accès dès le lendemain.

Il faut souligner **qu'il ne s'agit pas ici d'un piratage** d'une base de données. On ne sait pas combien de temps ni qui a pu avoir accès à cette quantité massive de données. Cependant, sur Internet, 24 heures suffisent pour que des robots (crawlers) aspirent l'intégralité d'une base de données non protégée.

Qui est concerné ?

On l'a dit, au niveau de la France, ce sont **52 millions de comptes** qui sont concernés sur le milliard de comptes compris dans la base de données. Il ne s'agit pas d'un piratage, on ne sait donc pas si les données ont réellement été volées ou non.

Surtout, on ne connait pas la liste des banques et services qui utilisent IDMerit comme prestataire pour la vérification des données. IDMerit est un service B2B, on ne rencontre pas son logo au moment de la création du compte.

Pour que 52 millions de comptes soient concernés en France, on peut toutefois supposer que la société est le partenaire de grandes banques en France.

Les bons réflexes

Si vous avez été victime d'un piratage ou d'une fuite de données, quelques bonnes pratiques sont à garder en tête pour mieux vous protéger. *Frandroid* en a fait une liste :

- Changer sans attendre les mots de passe des comptes concernés ;
- En profiter pour changer aussi les mots de passe identiques ou similaires sur d'autres services ;
- Utiliser des mots de passe uniques et solides (avec, pourquoi pas, un gestionnaire de mots de passe) ;
- Activer la double authentification (2FA) partout où c'est possible ;
- Activer les Passkeys quand c'est possible ;
- Dans les semaines à venir, se méfier des emails, SMS ou appels suspects, même s'ils semblent crédibles ;
- Ne jamais cliquer sur un lien ou télécharger une pièce jointe en cas de doute ;
- Prévenir ses contacts si le piratage peut les concerner ;
- Mettre à jour ses appareils et logiciels pour corriger d'éventuelles failles de sécurité ;
- En cas de virements frauduleux, faire un signalement sur la plateforme Perceval.

Utilisez-vous Google News (Actualités en France) ? Vous pouvez suivre vos médias favoris. Suivez **Frandroid sur Google News** (et Numerama).

Signaler une erreur dans le texte

Sources : 01net, Bonjourlafuite

PARTAGER

Banque en ligne · # Intelligence artificielle · # Servic…

Cassim Montilla | Journaliste - Chef de rubrique actualités

Votre enfant réclame un…
Il se fait pirater deux fois sa PS5…
Plus de 700 modèl d'imprima touchés…
Windows 11 : une faille critique…
Faille majeure dans le jeu vidé…
Des VPN disponible sur les stores…

VOITURES HYBRIDES >
Voici la consommation réelle et scandaleuse des hybrides rechargeables vendues en Europe : 30 marques passées au crible, Porsche et Toyota à l'opposé
20 février 2026 · 12:19

BONS PLANS >
Cette batterie externe de 10 000 mAh, compatible MagSafe, est bradée à -33 % sur Amazon
20 février 2026 · 12:19

GOOGLE >
3 raisons de craquer pour le tout nouveau Google Pixel 10a avant le 18 mars sur le Google Store
20 février 2026 · 12:11

Mobile + fibre : voici le combo parfait pour réduire vos factures sans sacrifier votre confort

GOOGLE >
Google Chrome améliore votre productivité avec trois nouvelles options très pratiques
20 février 2026 · 12:00

MICROSOFT >
Windows 11 : le Bloc-notes s'apprête à recevoir une mise à jour historique
20 février 2026 · 11:57

BONS PLANS >
Xiaomi Poco X7 : notre coup de coeur perd 40 % de son prix dans version 512 Go
20 février 2026 · 11:33

RENAULT >
Voitures électriques : le plan choc de Renault pour faire chuter les coûts de 40 %
20 février 2026 · 11:25

SPECIALIZED >
850 W et 111 Nm de couple : Specialized booste gratuitement la puissance de ses vélos électriques
20 février 2026 · 11:07

MONTRES CONNECTÉES >
Strava ajoute enfin ces cinq sports très demandés à son application
20 février 2026 · 11:06

TESLA >
Trahi par une publication officielle, Tesla confirme que ses voitures autonomes ne sont pas des voitures autonomes
20 février 2026 · 10:46