DIVULGATION COORDONNÉE · ISO/IEC 29147

Politique de divulgation responsable des vulnérabilités

Comment signaler à REVIEWIT SAS une vulnérabilité de ses sites ou de la solution REVIEWIT, ce que nous attendons des personnes qui nous la signalent et ce à quoi nous nous engageons en retour.

VERSION
1.0 · Novembre 2026

PÉRIMÈTRE
Domaine we-reviewit.com · solution SaaS REVIEWIT

DIFFUSION
Public

SOMMAIRE

01 Périmètre
02 Comment nous signaler une vulnérabilité
03 Ce que nous attendons de vous
04 Nos engagements et nos délais
05 Divulgation coordonnée et information des clients
06 Engagement de bonne foi

OBJET

La sécurité de la solution REVIEWIT et des données que nos clients nous confient est notre priorité. Si vous pensez avoir découvert une vulnérabilité, nous voulons l'apprendre de vous, la corriger vite et vous tenir informé. La présente politique s'inspire des pratiques de la norme ISO/IEC 29147 (divulgation des vulnérabilités). Les délais qu'elle indique sont ceux de notre procédure interne de gestion des vulnérabilités.

SECTION 01 Périmètre

DANS LE PÉRIMÈTRE

- Le domaine **we-reviewit.com** et ses sous-domaines exploités par REVIEWIT SAS : site public, Trust Center, consoles et interfaces de programmation (API) de la solution.
- La solution SaaS REVIEWIT, dans toutes ses régions d'hébergement, y compris l'assistant RITA et les connecteurs de collecte.

HORS PÉRIMÈTRE

- Les services de tiers, même utilisés par REVIEWIT ou raccordés à la solution (fournisseur d'identité d'un client, prestataires de REVIEWIT) : signalez-les à leur éditeur.
- Les données et les souscriptions d'autres clients ou d'autres personnes que vous.
- Le déni de service, les tests de charge, l'ingénierie sociale, l'hameçonnage et toute atteinte physique.
- Les constats sans impact de sécurité démontré : rapport brut d'un outil automatique, version de logiciel affichée, en-tête informatif manquant sans scénario d'exploitation.

SECTION 02 Comment nous signaler une vulnérabilité

Écrivez à **security@we-reviewit.com**, en français ou en anglais. Pour que nous puissions qualifier rapidement votre signalement, indiquez si possible :

- le site, la console ou l'API concerné, avec l'adresse ou le point d'accès exact ;
- la nature de la vulnérabilité et son impact possible ;
- les étapes qui permettent de la reproduire, avec une preuve de concept minimale ;
- la date de votre découverte et le moyen de vous recontacter.

Ne joignez à votre message aucune donnée personnelle ni aucune donnée d'un client que vous auriez pu voir : décrivez-la sans la copier. Les informations que vous nous transmettez, y compris vos coordonnées, ne servent qu'au traitement de votre signalement et ne sont communiquées à personne sans votre accord, sauf obligation légale (question sur vos données : **dpo@we-reviewit.com**).

SECTION 03 Ce que nous attendons de vous

- Agir de bonne foi et rester dans le périmètre de la section 01.
- Utiliser uniquement vos propres comptes ou des comptes de test, et n'accéder qu'au strict nécessaire pour démontrer la vulnérabilité ; vous arrêter dès qu'elle est démontrée.
- Ne consulter, modifier, supprimer ni extraire aucune donnée qui ne vous appartient pas. Si vous y accédez par accident, arrêtez-vous, prévenez-nous et effacez ce que vous auriez conservé.
- Ne pas dégrader le service : pas de déni de service, pas d'envoi massif de requêtes, de formulaires ou de messages, pas de logiciel malveillant, pas de maintien d'un accès ni de rebond vers d'autres systèmes.
- Nous signaler la vulnérabilité sans délai et ne pas la divulguer à des tiers avant sa correction et avant d'en avoir convenu avec nous (section 05).
- Ne demander aucune contrepartie en échange de votre signalement ou de votre silence.

SECTION 04 Nos engagements et nos délais

Les délais de correction courent à compter de la qualification, c'est-à-dire de notre évaluation de la gravité et de l'exploitabilité de la vulnérabilité dans notre contexte. La gravité suit la note CVSS de l'avis ou de notre évaluation.

ÉTAPE	ENGAGEMENT
Relève de la boîte	La boîte **security@we-reviewit.com** est relevée chaque jour, 7 jours sur 7.

ÉTAPE	ENGAGEMENT
Accusé de réception	Au plus tard deux jours ouvrés après la réception du signalement.
Qualification	Au plus tard deux jours ouvrés après la réception du signalement. Nous vous indiquons si le signalement est retenu.
Vulnérabilité critique	CVSS 9,0 ou plus, ou exploitation active connue quelle que soit la note : correction ou atténuation sous 14 jours.
Vulnérabilité élevée	CVSS 7,0 à 8,9 : correction ou atténuation sous 30 jours.
Vulnérabilité moyenne	CVSS 4,0 à 6,9 : correction sous 90 jours.
Vulnérabilité faible	Correction dans la prochaine publication planifiée.
Clôture	La correction est vérifiée par une nouvelle analyse ; nous vous informons de sa mise en service.

Chaque signalement retenu est inscrit à notre registre des vulnérabilités et suivi jusqu'à sa clôture. Nous ne publions jamais le détail d'une vulnérabilité qui n'est pas corrigée.

SECTION 05 Divulgation coordonnée et information des clients

- Une fois la vulnérabilité corrigée, vous pouvez publier vos travaux à une date convenue avec nous, sans données de clients ni éléments permettant d'attaquer une installation non corrigée.
- Nos clients sont informés selon leurs engagements contractuels. Lorsqu'une vulnérabilité exploitée entraîne une violation de données à caractère personnel, la violation est notifiée aux clients concernés au plus tard 24 heures après sa prise de connaissance.
- Lorsqu'une vulnérabilité exploitable ne peut pas être corrigée dans le délai, les clients concernés en sont informés, avec les mesures d'atténuation appliquées.

SECTION 06 Engagement de bonne foi

REVIEWIT SAS n'engagera aucune poursuite et ne déposera aucune plainte contre une personne qui a mené de bonne foi une recherche dans le respect de la présente politique et nous en a signalé les résultats sans délai. Cet engagement ne vaut que pour REVIEWIT SAS ; il ne lie ni ses clients ni ses prestataires.

Vous pouvez également signaler une vulnérabilité à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), selon l'article L. 2321-4 du code de la défense.

Pas de programme de prime. REVIEWIT SAS n'a pas de programme de prime aux bogues et ne verse aucune rémunération pour un signalement.

REVIEWIT SAS · Sécurité : **security@we-reviewit.com** · Délégué à la protection des données : **dpo@we-reviewit.com**. Politique revue au moins une fois par an. Version 1.0 · Novembre 2026 · la version française fait foi.