Google et Anthropic à 30 jours : qui porte le délai

Le 13 novembre 2026, Project Zero, l'équipe de recherche en sécurité de Google, a annoncé qu'à partir de janvier 2028 les failles qu'elle découvre seraient publiées 30 jours après leur signalement. Anthropic a suivi trois jours plus tard. Le délai de divulgation (temps laissé à un éditeur avant que les détails d'une faille deviennent publics) a été raconté comme une course entre l'IA et des mainteneurs épuisés. Il révèle autre chose : une règle réécrite par ceux qui trouvent, dont la charge retombe sur ceux qui corrigent puis déploient.

Par Alexandre Berge · 22 novembre 2026 · 13 min de lecture · Chronique

Une règle des années 2010 réécrite en trois jours

À la date du 21 novembre 2026, les faits sont établis par les textes des deux organisations. Le 13 novembre, Natalie Silvanovich, chercheuse de Project Zero, publie « Policy and Disclosure: 2026 Edition ». Depuis 2021, l'équipe appliquait une règle dite « 90 + 30 ». L'éditeur disposait de 90 jours pour corriger, puis de 30 jours de « soak time » (temps laissé aux utilisateurs pour installer le correctif) avant la publication des détails. La nouvelle politique publie la faille un nombre fixe de jours après son signalement, qu'elle soit corrigée ou non. Ce délai vaut 90 jours depuis le 13 novembre 2026, 60 à partir du 2 février 2027 et 30 à partir du 3 janvier 2028. La période de grâce disparaît, avec la plupart des cas particuliers. Ne subsistent que les failles déjà exploitées, celles rendues publiques par d'autres et la demande de l'éditeur, plus des exceptions rares, comme naguère pour Spectre et Meltdown.

Le 16 novembre, l'équipe Frontier Red Team d'Anthropic publie ses propres échéances. Pour les failles signalées à partir du 1er janvier 2027, le délai passe de 90 à 30 jours pour les failles de gravité élevée ou critique, et à 45 jours pour les autres. L'entreprise vise à saisir un coordinateur externe après 15 jours de silence d'un mainteneur (le responsable, bénévole ou salarié, d'un logiciel libre), au lieu de 30. Les détails techniques complets seront publiés 30 jours après la disponibilité d'un correctif, au lieu de 45. Le délai de sept jours pour les failles activement exploitées ne change pas. Des calendriers négociés restent possibles pour les logiciels difficiles à déployer, comme ceux des infrastructures critiques, et pour les failles qui exigent de modifier une spécification.

Les deux textes invoquent la même cause. Project Zero écrit que les grands modèles de langage ont accéléré la découverte et l'exploitation des failles, au point qu'un attaquant peut déduire presque aussitôt une faille de son correctif. Anthropic rappelle que les normes

existantes supposaient des correctifs avançant à vitesse humaine et des redécouvertes indépendantes improbables, et tranche : « Neither assumption holds today » (aucune de ces hypothèses ne tient aujourd'hui).

Le récit dominant oppose la vitesse des machines à l'épuisement des bénévoles

La couverture a raconté l'annonce comme un duel. D'un côté, la nécessité technique : Next, le 17 novembre, décrit un changement « dicté, sans surprise, par l'utilisation désormais générale de l'IA ». De l'autre, la fatigue. Le chercheur Marcus Hutchins, cité par ITPro le 18 novembre, prévient que « eventually, the software maintainers are just going to burn out and give up » (les mainteneurs finiront par s'épuiser et abandonner). Next rapporte que VideoLAN a rappelé que le déploiement posait autant de difficultés que la correction. En face, Natalie Silvanovich a fait valoir que chaque bug signalé en 2026 à un projet maintenu par des bénévoles avait été corrigé en moins de 30 jours, à une exception près, corrigée en 31 jours. Un porte-parole de Google a déclaré à Dark Reading que les éditeurs consultés jugeaient, dans l'ensemble, ces délais atteignables.

Ce récit a le mérite de la clarté. Il a le défaut de tout ramener à une affaire de vitesse et de bonne volonté : les bénévoles suivront, ou ne suivront pas. Il laisse dans l'ombre la manière dont le délai est construit, et qui en porte le reste une fois l'échéance passée.

Le délai suit le rythme de celui qui trouve, pas la capacité de celui qui corrige

Le texte de Project Zero contient l'aveu le plus éclairant de l'épisode. L'équipe y écrit trouver désormais « several vulnerabilities a week » (plusieurs failles par semaine) dans des cibles où elle en trouvait quelques-unes par an. La règle des 90 jours avait été calibrée pour ce second monde. Le changement d'échelle ne porte donc pas sur le délai accordé à chaque faille. Il porte sur le volume adressé au même correcteur, dans le même calendrier.

Le tableau de bord d'Anthropic donne l'ordre de grandeur de l'écart. Au 2 novembre 2026, l'entreprise y recense 5 087 failles signalées aux mainteneurs de projets libres, 3 635 accusées de réception et 629 corrigées en amont à sa connaissance. Ce dernier chiffre est un décompte déclaratif, qui ne dit rien de l'installation effective des correctifs. Les éditeurs d'IA ne comblent pas non plus l'écart eux-mêmes, selon Katie Moussouris, dirigeante de Luta Security et pionnière de la divulgation coordonnée, interrogée par Dark Reading : « A deadline doesn't magically manifest a fix » (une échéance ne fait pas apparaître un correctif par magie). Trail of Bits, partenaire de l'initiative d'OpenAI, a indiqué au même titre avoir écrit 733 correctifs pour 2 162 problèmes trouvés, dont 506 acceptés en amont. Un rapport de un à huit entre signalé et corrigé ne décrit pas une mauvaise volonté. Il décrit une capacité de traitement saturée. **Le délai raccourci ne crée aucune heure de travail chez le mainteneur. Il fixe seulement la date à laquelle le stock non traité devient public.**

Les éditeurs consultés par Project Zero l'ont dit autrement, et l'équipe le rapporte loyalement.

Un délai trop agressif inciterait à traiter en priorité les failles signalées par Project Zero, même moins graves que d'autres, et des éditeurs incapables de tenir l'échéance pourraient renoncer à essayer. L'émetteur de l'échéance réordonne ainsi la file d'attente du correcteur. **La priorité ne suit plus le risque, mais la provenance du signalement.**

Reste l'aval. Le compteur de Project Zero part désormais du signalement à l'éditeur, et non plus de la sortie du correctif. La suppression des 30 jours de « soak time » reporte le temps de déploiement sur l'éditeur, puis sur ceux qui installent : directions informatiques, collectivités, exploitants d'infrastructures. Project Zero nomme ce temps « patch gap » (l'intervalle entre la sortie d'un correctif et son installation) et demande aux éditeurs de le réduire. Rien, dans la politique, ne porte sur le calendrier de qualification d'un hôpital ou d'une préfecture.

> **Le concept, en une définition.**
>
> *L'asymétrie entre attaque et défense* (Ross Anderson, « Why Information Security is Hard – An Economic Perspective », 2001). Anderson soutient que l'insécurité tient au moins autant à des incitations perverses qu'à des défauts techniques. Dans un système vaste et complexe, un attaquant aux moyens modestes trouve une faille avant que le défenseur, même bien doté, ait trouvé la même : « Attack is simply easier than defense » (l'attaque est tout simplement plus facile que la défense). Le même texte énonce le corollaire organisationnel. Lorsque la partie en position de protéger un système n'est pas celle qui subirait la défaillance, des problèmes sont à prévoir.

Anderson avait décrit l'avalanche de rapports

L'article d'Anderson, présenté à la conférence ACSAC en décembre 2001, contient une parabole qui se lit aujourd'hui comme un compte rendu. Un attaquant isolé dispose de 1 000 heures de test par an, un défenseur de 10 millions. Au bout d'un an, le premier a trouvé une faille et le second 100 000, mais la probabilité que le défenseur ait trouvé celle de l'attaquant n'est que de 10 %. Anderson ajoute que les rapports du défenseur seront devenus un tel flot que Microsoft aura fini par les filtrer d'office.

La situation de 2026 reproduit cette parabole à une autre échelle. Les modèles d'IA démultiplient la découverte, chez les chercheurs comme chez les attaquants. Ce qu'Anderson tenait pour constant n'a pas bougé : la correction reste un travail humain, mené projet par projet. **L'asymétrie ne se joue donc plus seulement entre attaquant et défenseur. Elle traverse le camp de la défense lui-même, entre ceux qui trouvent à l'échelle industrielle et ceux qui corrigent à l'échelle artisanale.**

Le second apport d'Anderson nomme le transfert. Il parle de *liability dumping* (le report du risque sur une autre partie). Le délai de divulgation en est un instrument. Google et Anthropic exposent leurs raisons avec soin, et rien n'autorise à leur prêter une intention. La structure,

elle, est lisible : l'organisation qui fixe l'échéance ne supporte ni le coût de la correction ni celui de l'exposition. Anthropic reconnaît que des délais plus courts peuvent accroître la pression sur les mainteneurs. En contrepartie, l'entreprise propose de joindre des correctifs aux rapports lorsque c'est possible, d'analyser gratuitement le code des projets critiques et d'offrir six mois d'abonnement aux mainteneurs éligibles. La compensation est réelle. Elle prend la forme d'outils de l'émetteur, pas d'heures de correcteur.

Heartbleed, ou la dépendance découverte le jour de la faille

Le 7 avril 2014, OpenSSL, bibliothèque libre de chiffrement, publie un avis sur la faille CVE-2014-0160, aussitôt nommée Heartbleed. La note VU#720951 du CERT/CC en attribue la découverte à des chercheurs de Codenomicon et de Google. Le 12 avril, Steve Marquess, chargé des finances de l'OpenSSL Software Foundation, publie un texte qui déplace la question. La fondation recevait, selon lui, environ 2 000 dollars de dons directs par an. Un seul membre de l'équipe travaillait à plein temps sur OpenSSL, alors qu'il en aurait fallu au moins une demi-douzaine. Pour Marquess, le mystère n'était pas que quelques bénévoles surmenés aient manqué ce bug : « the mystery is why it hasn't happened more often » (le mystère est que cela ne soit pas arrivé plus souvent). Le 24 avril, rapporte The Register, la Linux Foundation lance avec treize entreprises, dont Google, Microsoft et Amazon Web Services, la Core Infrastructure Initiative. Ce programme, doté de plusieurs millions de dollars sans montant exact divulgué, prend OpenSSL pour premier chantier.

La proximité structurelle est nette. En 2014 comme en 2026, l'événement visible est technique (une faille, un délai). La question réelle porte sur la capacité de correction d'un maillon dont tout le monde dépend sans l'avoir comptée. La différence tient au sens du mouvement. En 2014, l'écosystème a découvert après coup qu'il sous-finançait ses correcteurs. En 2026, il accélère le rythme des signalements avant d'avoir mesuré la capacité qui doit les absorber. L'histoire de la règle elle-même va dans ce sens. En février 2015, selon Le Monde Informatique, Project Zero ajoutait une période de grâce de 14 jours à ses 90 jours, après avoir publié des failles de Windows peu avant leurs correctifs. L'échéance s'était alors ajustée à la capacité de l'éditeur.

Partout où un tiers fixe l'échéance et un autre porte la charge

Le mécanisme, sans les marques, tient en une phrase. Quand celui qui produit les signalements fixe seul le délai de traitement, et que sa capacité de production croît plus vite que la capacité de traitement du destinataire, l'écart devient un stock de risque. L'émetteur fixe la date de sa publication, le destinataire en supporte le coût.

Le mécanisme se reproduit à trois conditions. La première est un découplage entre la capacité de détection, qui s'industrialise, et la capacité de traitement, qui reste humaine et dispersée. La deuxième est une échéance unique, fixée par l'émetteur, sans référence au

volume total adressé au même destinataire. La troisième est un aval non compté : le délai mesure la remise d'un correctif, pas son installation par ceux qui exploitent.

Ces conditions débordent la sécurité informatique. Elles valent pour un audit interne qui multiplie les constats grâce à l'analyse automatique face à des équipes métier inchangées. Elles valent pour un régulateur qui raccourcit des délais de mise en conformité, ou pour un éditeur qui impose une montée de version à date fixe. Les signes sont observables : un indicateur qui compte les signalements émis et ignore les corrections installées, une file d'attente dont l'ordre suit la provenance plus que la gravité, des responsables qui ferment des canaux de réception pour tenir. Selon Next, le projet curl rend publics depuis le 26 octobre 2026 ses signalements de gravité faible et moyenne. GNOME a ramené son propre délai de 90 à 30 jours pour les failles signalées à partir du 1er août 2026. Michael Catanzaro, qui suivait ses failles depuis 2020, avait annoncé cesser de prendre en charge les nouveaux signalements au 1er novembre, alors que, rapportait Help Net Security, « No one else currently tracks GNOME security issues » (personne d'autre ne suit actuellement les failles de GNOME).

> **Grille de lecture**
>
> 1. Qui fixe, dans l'organisation, les délais de traitement des constats de sécurité, d'audit ou de conformité, et cette instance supporte-t-elle la charge de correction ?
> 2. Le volume de constats reçus par chaque équipe corrective sur les douze derniers mois est-il connu et rapporté à sa capacité ?
> 3. Les tableaux de bord mesurent-ils les correctifs installés, ou seulement les signalements émis et les correctifs livrés ?
> 4. Quelle part des composants critiques dépend d'un mainteneur extérieur dont l'effectif est connu ?
> 5. Lorsque deux constats arrivent ensemble, l'ordre de traitement suit-il la gravité ou l'identité de l'émetteur ?

Le calendrier est public, la capacité ne l'est pas

Google et Anthropic ont publié des dates précises, et c'est ce qui rend la lecture vérifiable. Le délai de 30 jours a été présenté comme l'adaptation d'une règle humaine à la vitesse des machines. Il est aussi le déplacement d'une charge : ceux qui trouvent fixent l'heure, ceux qui corrigent et déploient paient le temps. L'asymétrie qu'Anderson situait entre attaquant et défenseur passe désormais à l'intérieur de la défense.

Si cette lecture est juste, deux signes devraient être lisibles avant le 3 janvier 2028, date du passage de Project Zero à 30 jours. Sur le tableau de bord d'Anthropic, la part des failles corrigées parmi les failles signalées ne devrait pas rattraper le rythme des signalements, malgré le raccourcissement du 1er janvier 2027. Et d'autres projets libres devraient suivre curl et GNOME, en rendant publics leurs signalements de moindre gravité ou en cessant de les

trier. Si l'écart se referme au contraire sans départ de mainteneurs, l'argument de Natalie Silvanovich l'aura emporté : la contrainte aura créé la capacité.

Note méthodologique

Les faits reposent sur les textes publiés par Project Zero le 13 novembre 2026 et par Anthropic le 16 novembre 2026, recoupés par Next, Dark Reading et ITPro. Dark Reading décrit une baisse « de 120 à 30 jours » en comptant la période d'installation des correctifs dans l'ancien délai. L'article retient la présentation des textes officiels (90 jours plus 30). Le lien entre progrès de l'IA et raccourcissement des délais est assumé, parce que les deux organisations le revendiquent. L'effet sur les mainteneurs reste attribué à ceux qui l'expriment, et les chiffres d'Anthropic et de Trail of Bits sont présentés comme déclaratifs. Les faits sont arrêtés au 21 novembre 2026. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Documents des organisations et des autorités

Natalie Silvanovich, Google Project Zero, « Policy and Disclosure: 2026 Edition », 13 novembre 2026. https://projectzero.google/2026/11/disclosure-policy.html

Anthropic, Frontier Red Team, « Updating our coordinated vulnerability disclosure policy timelines », 16 novembre 2026. https://www.anthropic.com/research/coordinated-vulnerability-disclosure-timelines

Anthropic, « Anthropic's coordinated vulnerability disclosure dashboard », chiffres arrêtés au 2 novembre 2026, consulté le 21 novembre 2026. https://red.anthropic.com/2026/cvd/

Presse de référence

Vincent Hermann, Next, « Sécurité : Google et Anthropic vont dévoiler les détails des failles après 30 jours », 17 novembre 2026. https://next.ink/268034/securite-google-et-anthropic-vont-devoiler-les-details-des-failles-apres-30-jours/

Alexander Culafi, Dark Reading, « Google Project Zero Slashes Bug Disclosure Deadlines, Splitting Experts », 16 novembre 2026, mis à jour le 18 novembre 2026. https://www.darkreading.com/vulnerabilities-threats/google-project-zero-bug-disclosure-deadlines

Adam Shepherd, ITPro, « Companies will be given 30-day patch deadlines as researchers tighten bug disclosure windows », 18 novembre 2026. https://www.itpro.com/security/companies-will-be-given-30-day-patch-deadlines-as-researchers-tighten-bug-disclosure-windows

Ionut Arghire, SecurityWeek, « Google Project Zero Sets Course for 30-Day Disclosure Deadline », 16 novembre 2026. https://www.securityweek.com/google-project-zero-sets-course-for-30-day-disclosure-deadline/

Help Net Security, « AI-generated reports push GNOME to shorten its disclosure window », 21 juillet 2026. https://www.helpnetsecurity.com/2026/07/21/gnome-security-disclosure-update/

Cadre théorique

Ross Anderson, University of Cambridge Computer Laboratory, « Why Information Security is Hard – An Economic Perspective », communication à la 17th Annual Computer Security Applications Conference (ACSAC), décembre 2001, version de l'auteur consultée le 21 novembre 2026. https://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf

Parallèle historique

CERT/CC, Will Dormann, « OpenSSL TLS heartbeat extension read overflow discloses sensitive information », note VU#720951, 8 avril 2014. https://www.kb.cert.org/vuls/id/720951/

Steve Marquess, « Of Money, Responsibility, and Pride », blog Speeds and Feeds, 12 avril 2014. http://veridicalsystems.com/blog/of-money-responsibility-and-pride/index.html

Jack Clark, The Register, « Bevy of tech behemoths aim to plug the next Heartbleed with DOLLARS », 24 avril 2014. https://www.theregister.com/2014/04/24/linux_foundation_core_infrastructure

Le Monde Informatique, « Project Zero de Google assouplit sa politique de divulgation de failles », 16 février 2015. https://www.lemondeinformatique.fr/actualites/lire-project-zero-de-google-assouplit-sa-politique-de-divulgation-de-failles-60255.html