Politique de divulgation coordonnée des vulnérabilités de Nice / Politique publique

Nice prend très au sérieux la sécurité de ses produits et services numériques. Si vous pensez avoir identifié une faille de sécurité affectant un produit ou un service Nice, veuillez nous la signaler. Cette politique explique comment soumettre un rapport, les informations qui nous aident à l'évaluer et ce que vous pouvez attendre de notre part.

Comment signaler une vulnérabilité

1. Envoyez un e-mail à security@niceforyou.com. Indiquez un objet clair, par exemple : « Rapport de faille de sécurité – [produit ou service] ».
2. N'incluez pas de données personnelles superflues ni d'informations confidentielles appartenant à des tiers. Si vous souhaitez recevoir des mises à jour, indiquez un moyen de contact fiable.

Éléments à inclure

1. le produit ou service concerné, ou une description suffisante pour l'identifier ; le modèle, la version du micrologiciel/logiciel, la version de l'application ou l'URL du service peuvent être fournis s'ils sont connus ;
2. une description claire de la vulnérabilité présumée et, si vous les connaissez, son impact potentiel ;
3. les étapes nécessaires pour reproduire le problème et, le cas échéant, une preuve de concept ; ces éléments sont utiles mais ne sont pas obligatoires si le signalant ne peut pas les fournir ;
4. les conditions requises pour l'exploitation, y compris le vecteur d'attaque et les privilèges nécessaires, si ces informations sont connues ;
5. toute information indiquant que la vulnérabilité pourrait déjà faire l'objet d'une exploitation active ; si cela ne peut être déterminé, sélectionnez ou indiquez « inconnu/non observé ».

Ce que vous pouvez attendre de notre part

1. Nous nous efforçons d'accuser réception dans un délai de 3 jours ouvrés. Cet accusé de réception comprend le numéro de dossier et confirme uniquement la réception ; il ne constitue pas une validation de la vulnérabilité signalée.
2. Nous nous efforçons de fournir une première évaluation ou une mise à jour de l'état d'avancement dans un délai de 10 jours ouvrés.
3. Lorsque l'enquête est en cours et que vous avez fourni vos coordonnées, nous nous efforçons de vous fournir une mise à jour au moins tous les 30 jours, sauf si des raisons juridiques, de sécurité ou de confidentialité nous empêchent de partager certaines informations.

4. Il s’agit d’objectifs de service relatifs à la communication avec les signalants. Ils ne remplacent ni ne modifient les délais de signalement légaux applicables à Nice.

Divulgation coordonnée

Veuillez accorder à Nice un délai raisonnable pour enquêter et, le cas échéant, remédier au problème signalé avant de le rendre public. Nous nous efforcerons de coordonner toute divulgation avec vous, en tenant compte de la gravité de la vulnérabilité, de la disponibilité des mesures correctives, de la protection des utilisateurs et de toute obligation légale applicable. Le cas échéant et avec votre consentement, Nice pourra reconnaître publiquement votre contribution.

Recherche en matière de sécurité menée de bonne foi

Si vous menez des recherches en matière de sécurité de bonne foi et que vous respectez la présente politique, Nice n’engagera ni ne soutiendra aucune action en justice à votre encontre du seul fait de ces recherches. Cet engagement s’applique uniquement aux systèmes et activités relevant du champ d’application de la présente politique et de la compétence de Nice. Il ne lie pas les tiers et n’autorise pas les comportements illicites ou dépassant les limites définies ci-dessous.

Exigences en matière de recherche

1. ne tester que des produits, comptes, appareils ou systèmes dont vous êtes propriétaire ou que vous êtes expressément autorisé à tester ;
2. évitez toute atteinte à la vie privée et limitez au maximum l’accès aux données à caractère personnel ou aux informations confidentielles ;
3. interrompez les tests et prévenez-nous sans délai si vous accédez à des données qui ne sont pas nécessaires pour démontrer la vulnérabilité ;
4. ne pas conserver, modifier, supprimer, télécharger, copier, divulguer ou utiliser de quelque manière que ce soit les données appartenant à Nice, à ses utilisateurs ou à des tiers, à l’exception des informations minimales strictement nécessaires pour documenter la vulnérabilité ;
5. ne pas établir d’accès persistant, ne pas recourir à l’ingénierie sociale, ne pas menacer ni faire chanter, ne pas perturber les services, ni mener de tests de déni de service ou de tests volumétriques ;
6. ne pas exploiter la vulnérabilité au-delà de ce qui est strictement nécessaire pour la démontrer ; et
7. prévoyez un délai raisonnable pour l’enquête et la correction avant toute divulgation publique.

Champ d’application

La présente politique s’applique aux produits Nice comportant des éléments numériques qui se trouvent dans leur période de support déclarée, y compris les micrologiciels,

logiciels, applications mobiles et services cloud associés, ainsi qu'aux sites web ou services numériques exploités directement par Nice. Les signalements concernant des produits hors support peuvent néanmoins être soumis et seront évalués au cas par cas, sans que cela n'engage Nice à fournir une mise à jour corrective.

Sont exclus du champ d'application

1. les systèmes, produits ou services exploités exclusivement par des tiers, sauf si Nice a expressément autorisé leur inclusion ;
2. les attaques physiques, l'ingénierie sociale, le phishing ou les attaques visant des employés, des sous-traitants, des clients ou des fournisseurs ;
3. les attaques par déni de service, les attaques par déni de service distribué ou les tests susceptibles de nuire à la disponibilité ou aux performances ;
4. les tests automatisés générant un trafic excessif ou perturbant le fonctionnement normal du service ;
5. l'accès, la modification, la destruction, la conservation, l'extraction ou la divulgation de données au-delà de ce qui est strictement nécessaire pour démontrer la vulnérabilité ; et
6. les tests portant sur des produits, des comptes, des appareils ou des systèmes dont vous n'êtes pas propriétaire et que vous n'êtes pas autorisé à tester.

Signalements concernant des composants tiers

Si un rapport concerne un composant tiers intégré à un produit Nice, veuillez le signaler à Nice. Nous évaluerons le problème et, le cas échéant, coordonnerons notre action avec le fabricant, le fournisseur ou le responsable de la maintenance du composant concerné, conformément à notre processus interne de gestion des vulnérabilités.

Absence d'engagement en matière de programme de prime aux bogues

La présente politique ne donne lieu à aucun programme de prime aux bogues ni à aucun droit à un paiement, une récompense ou toute autre forme de compensation. Toute reconnaissance ou récompense doit faire l'objet d'un accord écrit explicite de la part de Nice.

Données à caractère personnel

Les données à caractère personnel fournies dans le cadre d'un rapport de vulnérabilité ne seront traitées que dans la mesure nécessaire pour recevoir, évaluer, examiner et gérer le rapport, communiquer avec le signalant, protéger Nice et ses utilisateurs, et respecter les obligations légales applicables. La déclaration de confidentialité applicable en vertu du règlement (UE) 2016/679 est disponible sur la page dédiée aux rapports de sécurité.