Étude de risques sur la sécurité des produits Red Hat 2023

Sommaire

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

Introduction

Si les années 2021 et 2022 ont été celles de la sécurité des chaînes d'approvisionnement, 2023 s'est caractérisée par un vif enthousiasme autour de l'intelligence artificielle (IA). Les avancées de l'IA générative et des grands modèles de langage (LLM) ont été des sujets récurrents, que ce soit dans les communiqués de presse techniques, les salles de réunion ou encore dans les forums. Qu'elle soit source d'admiration ou redoutée, l'IA progresse et impacte le monde doucement mais surement.

Face aux défis inédits et aux formidables possibilités que représente l'IA, l'équipe Red Hat® Product Security s'implique activement notamment par un travail de veille. Chez Red Hat, nous excellons à proposer des processus de développement axés sur la sécurité et la transparence des données au sein de plateformes de cloud hybride ouvert, et nous nous engageons à fournir aux clients des outils de prise de décision en matière de sécurité basés sur les risques.

Cette nouvelle étude de risques fournit un aperçu complet des principaux domaines de sécurité de Red Hat. Elle inclut des données clés et des statistiques issues de notre programme de gestion des vulnérabilités, une analyse approfondie de deux incidents majeurs de niveau Critique, ainsi que les dernières informations sur notre programme de développement sécurisé renforcé. Nous aborderons également l'évolution des chaînes d'approvisionnement des logiciels au cours de l'année passée. Enfin, nous terminerons par un message de notre vice-président, Vincent Danen.

Je suis convaincu que cette étude de risques, en parallèle de l'engagement sans faille de Red Hat en faveur de la transparence, sera utile à nos clients et à la communauté tout entière et leur apportera des données précieuses. Bonne lecture !

- Garth Mollett, architecte en chef de l'équipe Product Security, Red Hat

RHSA (Red Hat Security Advisory)

Créés il y a 20 ans, les avis de sécurité Red Hat Security Advisory restent aujourd'hui encore le principal mécanisme de notification en cas de publication d'une mise à jour de logiciel venant corriger des vulnérabilités identifiées dans le catalogue CVE (Common Vulnerabilities and Exposures). Malgré les changements apportés au fil du temps, notamment au niveau du format et du processus de distribution, l'objectif principal reste le même.

Comme prévu, la tendance à la hausse des avis de sécurité s'est poursuivie en 2023. L'augmentation constatée de 2022 à 2023 est similaire à ce que nous avons observé au cours des dernières années. Les fluctuations s'expliquent avant tout par la taille et la complexité des solutions, plus que par une tendance marquée en matière de sécurité, le nombre total de vulnérabilités signalées ayant baissé en réalité.

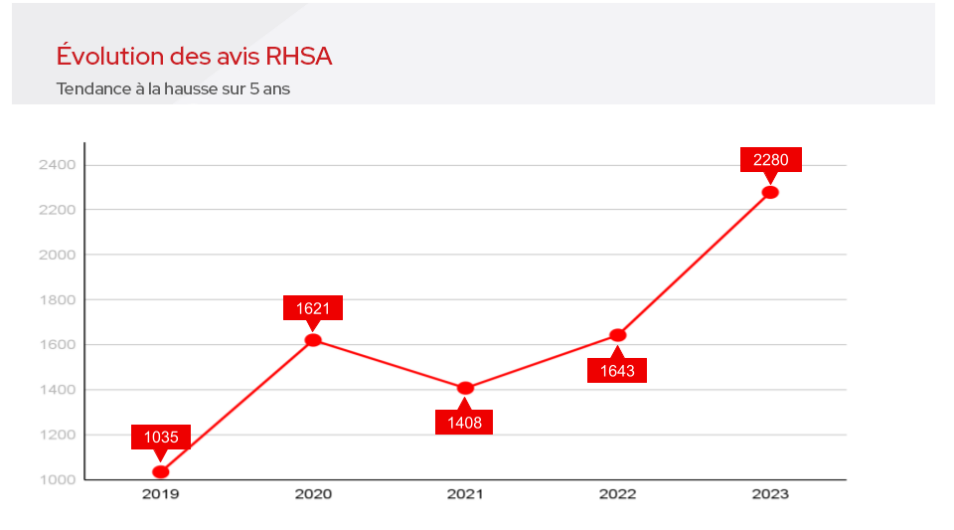


Figure 1 : évolution des avis RHSA

Tableau 1 : avis de sécurité RHSA par niveau de gravité

Total	2 280	+637 depuis 2022
Critique	65	+30 depuis 2022
Important	1 405	+512 depuis 2022
Modéré	760	+125 depuis 2022
Faible	50	-30 depuis 2022

CVE (Common Vulnerabilities and Exposures)

Les chiffres relatifs aux CVE demeurent assez stables. Leur nombre a légèrement diminué en 2023 par rapport à 2022, et reste toujours nettement inférieur au pic de 2020.

Alors que le nombre de vulnérabilités de niveau Critique est descendu à 12, les vulnérabilités de niveau Important ont fortement augmenté, ce qui explique sans doute l'augmentation des avis de sécurité Red Hat, les CVE de niveau Important étant rapidement corrigées. Les vulnérabilités de niveau Modéré, en hausse de 39 points, ont plus de chances d'être corrigées de façon groupée dans une version planifiée de plus grande ampleur.

Comme toujours ou presque, les CVE de niveau Modéré restent les plus fréquentes, le nombre de signalements de failles à impact modéré étant une fois de plus supérieur à toutes les autres catégories combinées.

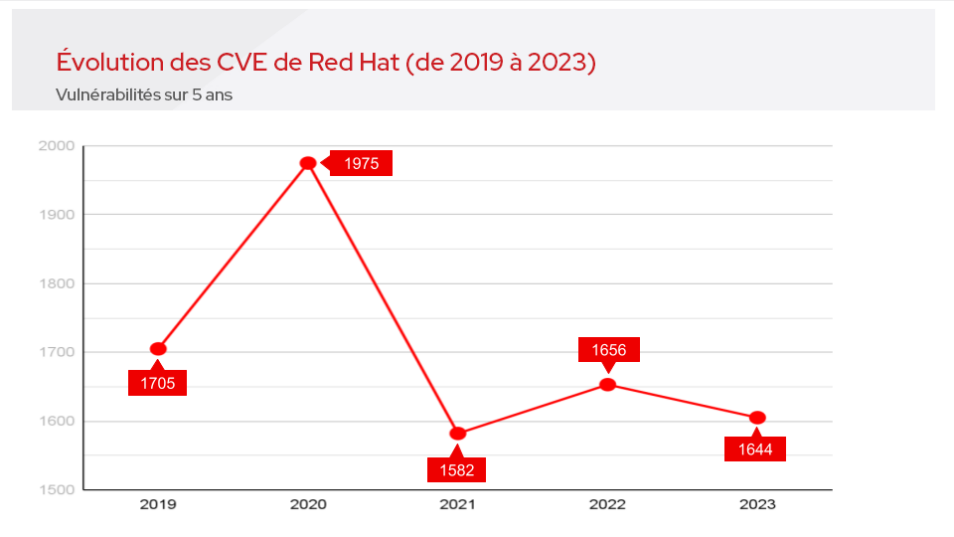


Figure 2 : évolution des CVE de Red Hat (de 2019 à 2023)

Tableau 2 : vue d'ensemble des failles de sécurité par niveau de gravité

Niveau de gravité	Nombre total de failles (chiffre approximatif depuis 2022)	Exploitations sauvages (% du total | chiffre approximatif depuis 2022)
Tous niveaux confondus	1 644 (-12)	20 (1,2 % | +13)
Critique	12 (-7)	1 (8,3 % | -1)
Important	336 (+60)	15 (4,5 % | +12)
Modéré	1 047 (-39)	3 (0,3 % | +1)
Faible	247 (-28)	1 (0,4 % | +1)

Sans surprise, l'augmentation des failles importantes se traduit par une hausse des exploitations sauvages.

Bien qu'il soit rassurant de voir que ces chiffres restent faibles, il importe de comprendre qu'une grande partie de ces informations, concernant des attaques réelles, reste confidentielle et n'est pas divulguée au public et aux fournisseurs. Par ailleurs, de nombreuses attaques passent inaperçues. Et lorsque celles-ci sont détectées, les petites entreprises n'ont souvent pas les moyens d'effectuer des analyses détaillées ou des diagnostics pour accéder à ces informations. La différence significative entre les CVE de niveau Faible et Modéré et les CVE de niveau Important ou Critique reflète en partie leur caractère exploitable et pertinent dans des scénarios d'attaques réels. Les chiffres réels sont probablement plus élevés et méritent des études poussées.

Délais de réponse

Le délai de réponse, c'est-à-dire la rapidité de publication d'un correctif, demeure une priorité pour l'équipe Red Hat Product Security ainsi que de nombreux clients. Si l'exploitation des vulnérabilités zero-day, encore inconnues des fournisseurs ou du public, reste une menace réelle émanant des cybercriminels les mieux financés, le délai de réponse entre la divulgation publique des informations sur la faille et l'application des correctifs représente le plus grand risque.

Avant leur application, les correctifs doivent être développés, testés et publiés. Lorsque nous participons au processus de divulgation coordonné, ces étapes ont lieu avant même que la vulnérabilité soit rendue publique. Dans tous les cas, nous réalisons des tests poussés avant publication pour rassurer les clients et alléger leur travail de test.

Pour des raisons de transparence, nous comparons ces chiffres à ceux publiés dans l'étude de l'année dernière pour la même période. Le délai de réponse moyen a légèrement augmenté pour toutes les vulnérabilités, sauf celles de gravité faible, ce qui peut paraître alarmant à première vue. En réalité, rapporté au faible nombre de vulnérabilités au total, ces moyennes peuvent être aisément biaisées par quelques failles plus difficiles ou plus longues à corriger. Bien que nous nous efforcions de maintenir cette tendance au plus bas niveau, des fluctuations mineures ne sont pas surprenantes, en particulier sur une période définie plutôt qu'en continu.

Tableau 3 : comparaison des temps d'exposition aux risques par niveau de gravité

Niveau de gravité	2022	2023	Évolution
Critique	6 jours	9 jours	50 % plus lent
Important	36 jours	48 jours	33 % plus lent
Modéré	108 jours	112 jours	4 % plus lent
Faible	168 jours	130 jours	23 % plus rapide

Analyse par produit

La majorité des avis de sécurité de niveau Important et Critique concernent toujours les trois versions majeures de Red Hat Enterprise Linux (versions 7 à 9). Cette statistique n'est pas surprenante compte tenu de la taille et de la complexité de ces distributions, ainsi que de la quantité de code C qu'elles contiennent. Cependant, l'écart entre Red Hat Enterprise Linux® et Red Hat OpenShift® se réduit, la plateforme OpenShift ayant fait l'objet de presque deux fois plus d'errata critiques.

Notez que le nombre de CVE correspond au nombre de failles CVE corrigées pour un errata donné, lequel n'est pas forcément critique ou important. Cette tendance est flagrante pour les produits de middleware. En effet, le regroupement de plusieurs correctifs dans les versions planifiées ou la correction des failles via le rebasage d'un composant sur une nouvelle version en amont implique d'intégrer plusieurs correctifs plutôt que de rétroporter un seul correctif dans une version existante, une démarche plus courante.

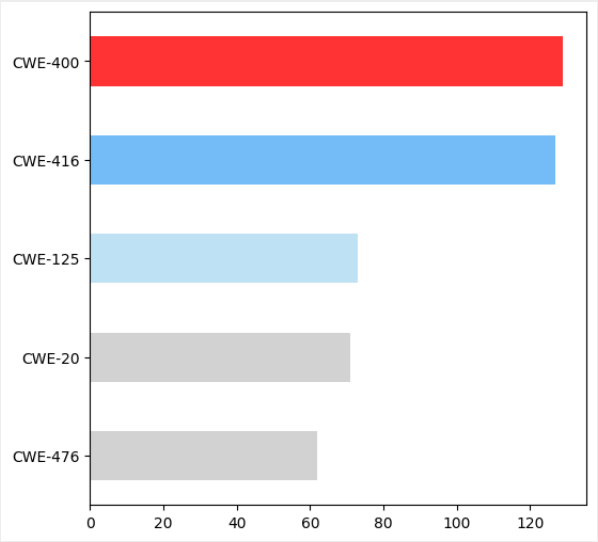
Tableau 4 : RHSA importants et critiques, et nombres de CVE, par produit

Produit	RHSA importants (nombre de CVE)	RHSA critiques (nombre de CVE)
Red Hat Enterprise Linux	978 (557)	18 (10)
Red Hat OpenShift	221 (231)	32 (64)
Red Hat Ansible® Automation Platform	5 (13)	0 (0)
Red Hat OpenStack® Platform	27 (35)	4 (1)
Produits de middleware	101 (175)	8 (48)
Red Hat Virtualization	18 (56)	0 (0)
Red Hat Satellite	8 (60)	2 (3)

CWE (Common Weakness Enumeration)

Pour les équipes dont la tâche est de comprendre les vulnérabilités des logiciels, plus que la gravité ou le nombre de failles dans les composants, c'est le type de failles observées et les exploitations sauvages fréquentes qu'il convient d'analyser.

Pour obtenir ces informations, il faut s'intéresser aux CWE. Cette liste dans laquelle sont classées les vulnérabilités respecte une catégorisation relativement basique. En effet, elle tient peu compte de la complexité des pipelines de développement des exploits modernes, où les cybercriminels combinent des primitives d'exploitation afin d'obtenir les capacités visées pour l'attaque. Si elles n'offrent qu'une vision partielle de la situation, les CWE s'avèrent néanmoins utiles pour comprendre où concentrer le travail de défense.



CWE-400
Consommation incontrôlée de ressources

CWE-416
Utilisation de zone désallouée

CWE-125
Lecture hors limites

CWE-20
Validation d'entrée incorrecte

CWE-476
Déréférencement d'un pointeur null

Figure 3 : les cinq principaux CWE en 2023

La consommation incontrôlée de ressources prend la première place cette année, de même que les failles observées lors des attaques « Rapid Reset » (mentionnées ultérieurement), qui connaissent un regain d'intérêt. Sans surprise, le reste du top 5 est occupé par des problèmes classiques et récurrents de corruption de la mémoire dus en grande partie à Red Hat Enterprise Linux et au code en langage C.

La situation est différente si l'on considère une période plus longue, depuis la première collecte de données CWE par l'équipe chargée de la résolution des incidents de sécurité des produits Red Hat en 2012, et que l'on se concentre sur les classes de vulnérabilités avec au moins cinq cas différents de bogues ayant fait l'objet d'une exploitation sauvage. Cependant, le CWE-416 (Utilisation de zone désallouée) tient le haut du classement, juste derrière le CWE-20 (Validation d'entrée incorrecte), une catégorie de failles plus large et générale que le CWE-416, bien plus spécifique.

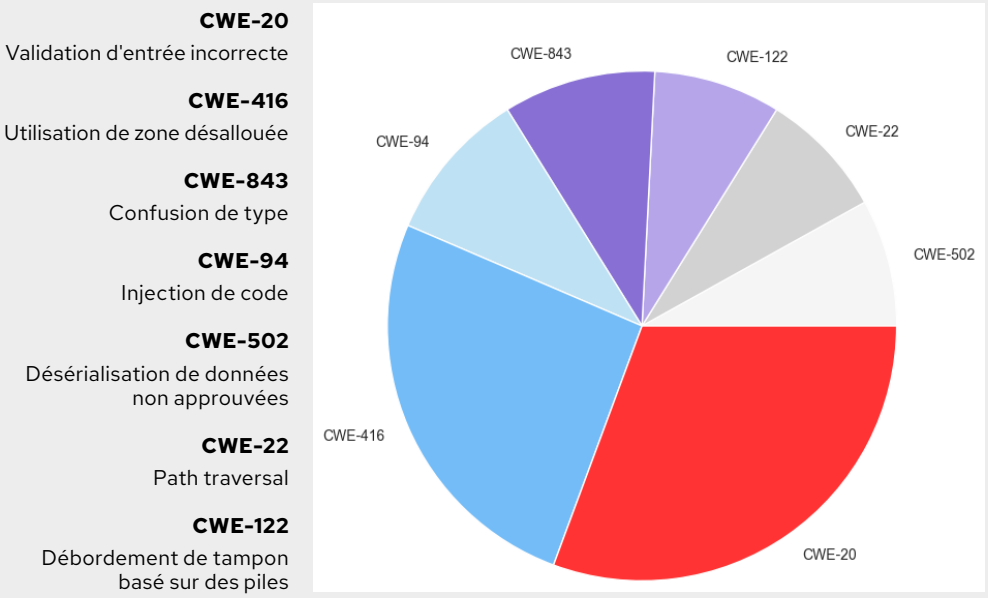


Figure 4 : CWE avec cinq cas ou plus d'exploitation sauvage depuis 2012

Exemples d'incidents majeurs

Dans le cadre du traitement des incidents majeurs, l'équipe Red Hat Product Security évalue l'éligibilité des vulnérabilités ou des événements selon différents facteurs. Le principal facteur est l'exposition aux risques, y compris aux risques perçus pour nos clients et notre marque. Les risques de sécurité liés à l'exploitation massive et triviale de logiciels essentiels sont considérés en premier. D'autres types de risques sont également pris en compte, comme ceux liés à la désinformation et à l'anxiété que génère une couverture médiatique vague ou excessive.

Le but du processus de réponse aux incidents majeurs n'est pas tant de hiérarchiser les correctifs (ce travail intervient dès lorsqu'un incident est classé comme critique ou important) que de maintenir ouverts des canaux de communication clairs, pondérés et précis, à la fois dans l'entreprise et avec la clientèle. Côté client, cela se traduit par l'émission d'artéfacts supplémentaires comme des bulletins de sécurité Red Hat (RHSB, pour Red Hat Security Bulletin), des règles de détection Red Hat Insights, des playbooks de correction Ansible, l'errata de sécurité habituel, ainsi que des entrées sur la page des CVE.

Cette section décrit deux des trois incidents majeurs ayant fait l'objet de bulletins de sécurité en 2023. Pour chacun d'entre eux, nous avions fourni les informations détaillées suivantes :

- Informations de base
- Informations détaillées (pour les personnes qui s'intéressent au mécanisme des vulnérabilités logicielles)
- Statistiques (les versions de produit concernées par exemple)
- Estimation du temps de résolution du problème par les équipes Red Hat
- Signalement d'une exploitation sauvage et heure exacte du signalement auprès des équipes Red Hat, le cas échéant

RHSB-2023-002 : contournement de la politique de sécurité Quarkus - Quarkus - CVE-2023-4853

Informations de base : vulnérabilité relativement simple et compréhensible. Le contrôle d'accès basé sur les chemins d'accès implémenté par la version Red Hat de Quarkus ne permettait pas de normaliser complètement les chemins de la même manière que la résolution du routage des requêtes HTTP. Ainsi, il était facile de contourner ce contrôle en ajoutant des barres obliques (« / ») aux chemins lors de l'interrogation d'une ressource protégée.

Informations détaillées : plusieurs composants de la version Red Hat de Quarkus ont permis de baser la politique de contrôle d'accès sur les chemins. Les composants concernés étaient les suivants : `QUARKUS-VERTEX-HTTP`, `QUARKUS-UNDERTOW`, `QUARKUS-CSRF-REACTIVE` et `QUARKUS-KEYCLOAK-AUTHORIZATION`. Les quatre composants contenaient des implémentations légèrement différentes du modèle décrit ci-avant, où la logique de mise en correspondance ne normalisait pas correctement les chemins d'accès avant comparaison. Il était donc possible de la contourner avec des chemins d'accès ne correspondant pas exactement à la définition de la politique, mais qui étaient assez normalisés pour accéder à la ressource protégée ciblée.

Statistiques

Versions majeures concernées : Red Hat OpenShift Serverless 1, version Red Hat de Apache Camel, version Red Hat de Quarkus, Red Hat Integration 2, Red Hat Process Automation Manager 7

Temps estimé pour les équipes : 1 024 heures

Niveau de gravité : Important

Durée de l'embargo : 0 jour

Temps écoulé entre la divulgation publique et la publication du premier correctif : 7 jours/1 009 jours (signalement problème de sécurité/bogue initial)

Temps écoulé entre la divulgation publique et la publication de l'ensemble des correctifs : 28 jours/1 092 jours (signalement problème de sécurité/bogue initial)

Publication du code d'exploit : NA. Aucun code requis pour l'exploit.

Exploitation sauvage : non signalée, mais probable à une certaine échelle.

Conclusion : cette vulnérabilité souligne deux choses. D'abord, elle montre à quel point la complexité peut entraver la sécurité. Ce qui semble être une tâche simple a priori (comparer des chemins d'accès) devient difficile en raison de la complexité de la plateforme et des différentes couches en jeu. Ensuite, il convient de souligner le délai important qui s'est écoulé entre le moment où la vulnérabilité a été rendue publique et la publication du correctif. Ce retard en amont tient à

l'appréciation incomplète des implications liées à la sécurité lors du premier signalement public effectué via un problème GitHub. Il a donc fallu déterminer s'il s'agissait d'un comportement attendu ou d'un problème avec la documentation. Lorsque le problème a de nouveau été signalé, près de trois ans plus tard, les répercussions ont été identifiées et les correctifs hiérarchisés.

RHSB-2023-003 : attaque HTTP/2 Rapid Reset CVE-2023-44487 et CVE-2023-39325

Informations de base : dans la dernière quinzaine du mois d'août, Amazon Web Services (AWS), Cloudflare et Google ont remarqué une saturation du service HTTP.

En examinant le trafic et l'attaque de plus près, ils ont découvert une nouvelle technique d'attaque qui consiste à abuser des caractéristiques du protocole HTTP/2 pour consommer beaucoup plus de ressources que le trafic lui-même.

Informations détaillées : le protocole HTTP/2 établit plusieurs flux de communication bidirectionnels sur une seule connexion TCP. La communication sur ces flux est multiplexée pour permettre l'exécution de plusieurs requêtes simultanées sur une seule connexion, sans avoir besoin d'établir plusieurs sessions TCP ou d'attendre qu'une requête soit finalisée pour passer à la suivante, comme c'est le cas avec les précédentes versions du protocole HTTP.

Il importe d'assurer le bon fonctionnement des machines à états finis pour chaque flux de manière bilatérale, comme pour la couche TCP où le protocole régit les transitions entre les états pour établir et interrompre les flux, transmettre et recevoir des données, et gérer les conditions d'erreur. Tout ceci est défini dans la spécification RFC HTTP/2 RFC9113 que nous allons résumer.

Pour que les clients et les serveurs s'entendent, le protocole fournit plusieurs paramètres configurables que ceux-ci peuvent s'échanger et qui leur permettent de s'accorder sur les paramètres les plus adaptés à la session. L'un de ces paramètres annonce le nombre maximal de flux qui pourront être initiés simultanément par l'autre partie (SETTINGS_MAX_CONCURRENT_STREAMS). Si l'un des points de terminaison tente d'initier un nouveau flux alors que la limite a été atteinte, la partie réceptrice doit rejeter la tentative en envoyant le code d'erreur PROTOCOL_ERROR ou REFUSED_STREAM dans une trame RST_STREAM.

Il est intéressant de se pencher sur l'interaction entre la machine à états finis, la trame RST_STREAM et le paramètre MAX_CONCURRENT_STREAMS. La machine présente cinq états : IDLE, RESERVED, OPEN, HALF-CLOSED et CLOSED. Seuls les flux à l'état OPEN et HALF-CLOSED sont comptabilisés dans MAX_CONCURRENT_STREAMS. Tout flux recevant une trame RST_STREAM passe à l'état CLOSED, peu importe son état initial. Il ne compte donc plus dans le total MAX_CONCURRENT_STREAMS.

Une fois ce mécanisme compris, l'attaque en elle-même est simple. Un point de terminaison client ouvre un nouveau flux en demandant une ressource, puis envoie immédiatement une trame RST_STREAM. Tout semble normal du point de vue de la machine à états finis, parce qu'elle n'existe pas en vase clos et qu'elle assure le transport de la communication. Lors de réception de la trame RST_STREAM et du passage à l'état CLOSED, la demande de ressource peut déjà être en file d'attente ou en cours de traitement, sur le point de terminaison ou bien souvent sur un autre système. Cela permet au client d'ouvrir un nouveau flux. Si cette action est répétée, la quantité de ressources utilisées sera importante quel que soit le paramètre MAX_CONCURRENT_STREAMS. Cette attaque menée via un petit botnet en août dernier a eu des répercussions sans précédent.

Statistiques :

Versions majeures concernées : comme il s'agissait d'une faille au niveau du protocole, presque tous les produits ont été concernés.

Temps estimé pour les équipes : plus de 6 000 heures

Niveau de gravité : Important

Durée de l'embargo : 1 jour

Temps écoulé entre la divulgation publique et la publication du premier correctif : 7 jours

Temps écoulé entre la divulgation publique et la publication de l'ensemble des correctifs : 22 jours

Publication du code d'exploit : oui

Exploitation sauvage : oui. Ce problème a été découvert suite à une attaque active sauvage et a été ajouté au catalogue des vulnérabilités exploitées connues (KEV) de l'agence américaine CISA le même mois.

Conclusion : il est rare qu'une faille sans conséquences sur la confidentialité ou l'intégrité d'un système constitue un incident majeur. C'était pourtant le cas avec l'attaque Rapid Reset. S'agissant d'une faille au niveau du protocole, un grand nombre de logiciels ont été touchés. Sa résolution a entraîné des coûts exorbitants, comme le montre l'estimation des heures de travail des équipes. En outre, cette faille a été décelée suite à une attaque en cours contre trois grands hyperscalers, qui ont dû déployer des efforts considérables pour se défendre, en plus de leurs activités quotidiennes déjà colossales.

Nous tenons à remercier particulièrement les équipes d'AWS, de Cloudflare et de Google Cloud Platform. En plus de bloquer l'attaque pour leurs clients, celles-ci ont aussi partagé des analyses techniques approfondies qui ont permis à la communauté Open Source de corriger plusieurs codes base concernés par la faille pour éviter que celle-ci ne puisse à nouveau être exploitée.

Développement sécurisé

Cette année, nous avons continué à mettre l'accent sur le développement sécurisé et normalisé davantage de pratiques liées au cycle de développement sécurisé. En prêtant une attention constante à ce processus, nous nous attachons essentiellement à réduire les risques pour nos clients. Nous ne respectons pas seulement les normes du secteur comme le SSDF (Secure Software Development Framework) du NIST, nous veillons à distribuer des produits et des services fiables. Cet engagement augmente la valeur de notre gamme de produits et renforce la confiance des clients dans notre marque.

Chez Red Hat, nous utilisons le modèle de développement Open Source pour favoriser l'innovation et mettre au point des technologies plus fiables et plus stables. Nous contribuons activement au test et au renforcement des logiciels Open Source en amont afin d'offrir une base plus solide à l'ensemble de nos clients. En aval, nous appliquons rigoureusement les meilleurs frameworks de développement sécurisé du secteur tels que le SSDF, dépassant ainsi les exigences de sécurité communes du NIST SP 800-53. Pour ce faire, nous alignons nos normes de sécurité internes rigoureuses sur le cadre NIST SP 800-218 (SSDF) et nous nous appuyons sur les contrôles du NIST SP 800-53.

Notre système exhaustif de contrôles de sécurité comprend des tests statiques et dynamiques de la sécurité des applications (SAST et DAST), la modélisation des menaces avec revues du code et de l'architecture, des tests d'intrusion via des analyses automatisées et des tests en boîte blanche.

Dans les sections suivantes, vous découvrirez ces activités en détail ainsi que nos principales réalisations en matière de sécurité, illustrées par des statistiques et des faits notables.

Modélisation des menaces

En 2023, nous avons mené 105 missions de modélisation des menaces, lesquelles ont permis d'identifier 310 faiblesses de mise en œuvre. Aucune de ces faiblesses n'a atteint le seuil requis pour être considérée comme une vulnérabilité ou comme pouvant engendrer une vulnérabilité. Cependant, certaines auraient sans doute entraîné des vulnérabilités si les produits n'avaient pas été renforcés.

Nous classons ces possibilités de renforcement sur une échelle similaire à celle des vulnérabilités, à savoir Faible, Modéré, Important et Critique, et y ajoutons le niveau Informatif. Le tableau ci-dessous indique le total pour chaque niveau.

Tableau 5 : faiblesses de mise en œuvre

Niveau de gravité	Total
Critique	8
Important	87
Modéré	102
Faible	79
Informatif	34

Tests d'intrusion

Notre équipe PenTest, rattachée au service Red Hat Product Security, a mené 39 tests d'intrusion en 2023. Ceux-ci ont révélé 101 faiblesses de mise en œuvre et 17 vulnérabilités exploitables allant de problèmes de niveau Informatif à des problèmes empêchant l'exécution du code à distance.

Tableau 6 : tests d'intrusion

Type	Niveau de gravité	Total
Vulnérabilité	Critique	2
Vulnérabilité	Important	2
Vulnérabilité	Modéré	9
Vulnérabilité	Faible	4
Faiblesse de mise en œuvre	Critique	2
Faiblesse de mise en œuvre	Important	4
Faiblesse de mise en œuvre	Modéré	10
Faiblesse de mise en œuvre	Faible	34
Faiblesse de mise en œuvre	Informatif	51

Tests dynamiques et rapides de la sécurité des applications (RapiDAST)

Initialement développé en 2021 pour notre équipe PenTest, l'outil de test de sécurité RapiDAST est aujourd'hui accessible à tous en Open Source via GitHub.

Avec RapiDAST, les utilisateurs peuvent configurer et exécuter divers outils d'analyse sur des points de terminaison d'API d'applications actives, en profitant de fonctions d'automatisation et de création de rapports. L'outil permet de générer des rapports dans des formats lisibles par l'homme et les machines et s'intègre à des solutions de reporting comme DefectDojo d'OWASP (Open Worldwide Application Security Project).

Bien que RapiDAST soit proposé sans assistance, toute contribution est la bienvenue, et nous continuerons à le développer à mesure que nous l'intégrerons dans nos pipelines de distribution.

Sécurité des chaînes d'approvisionnement

Notre équipe Red Hat Product Security a adopté une approche encore plus proactive pour renforcer la sécurité de notre chaîne d'approvisionnement des logiciels. En 2023, l'application de règles de sécurité strictes tout au long de la chaîne a permis de poser les bases de notre stratégie basée sur les risques.

Avant d'être intégré dans les pipelines de production, chaque système qui gère du code fait l'objet d'un processus rigoureux d'approbation des opérations de sécurité. Nous avons identifié ces systèmes et défini des processus pour combler les failles de sécurité, ce qui a permis de réduire de 20 % la dette technique par la mise hors service de ressources non essentielles. Ces actions limitent considérablement les risques de sécurité associés aux systèmes non corrigés et non gérés.

En 2023, dans la continuité de notre stratégie de sécurité des produits basée sur les risques, nous avons déployé des pratiques globales pour gérer les risques potentiels dans la chaîne d'approvisionnement (voir ci-dessous).

Tendances en matière de menaces

En 2023, The Linux Foundation a interrogé 691 entreprises concernant leur usage des technologies Open Source. Voici les trois technologies qui se dégagent : Linux (64 %), le cloud computing et les conteneurs (63 %), et les outils d'intégration et distribution/déploiement continus (CI/CD) et DevOps (54 %). Naturellement, cette forte dépendance vis-à-vis des technologies Open Source en font une cible parfaite pour les attaques contre les chaînes d'approvisionnement des logiciels.

Les menaces visant les chaînes d'approvisionnement auxquelles sont confrontés les éditeurs continuent d'augmenter, et le monde de l'Open Source n'y échappe pas.

Sur 52 attaques contre les chaînes d'approvisionnement rendues publiques en 2023, nous avons établi que **79 %** d'entre elles émanaient de cybercriminels inconnus (voir la *Figure 5 pour découvrir les cybercriminels connus*) et qu'il était impossible d'établir le motif de l'attaque dans **67 %** des cas. Voici les deux scénarios d'attaque les plus courants :

- **Scénario à faible probabilité et aux conséquences importantes :** attaques par un cybercriminel expérimenté et disposant de ressources conséquentes, qui affectent sérieusement la posture de sécurité d'une entreprise. Ce type d'attaque entraîne une altération du code avec des implications à grande échelle pour les chaînes d'approvisionnement des logiciels en amont et en aval.
  - Ces attaques représentent environ **17 %** des attaques contre les chaînes d'approvisionnement des logiciels rendues publiques en 2023.
  - L'attaque SolarWinds de 2020 en est l'exemple le plus célèbre.
  - L'exemple le plus récent est l'attaque menée contre l'application de bureau 3CX en mars 2023.

- **Scénario à forte probabilité et aux conséquences moindres :** attaques opportunistes par des cybercriminels plus ou moins expérimentés visant des cibles qui présentent des faiblesses faciles à exploiter, ou des vulnérabilités dans des écosystèmes Open Source qui reposent sur une chaîne d'approvisionnement des logiciels de plus en plus décentralisée. Qu'il s'agisse d'attaques ciblées ou non, les groupes cybercriminels et les cyberattaquants soutenus par des États exploitent les mêmes maillons faibles des chaînes d'approvisionnement des logiciels et utilisent des vecteurs d'attaque similaires. Leur ingéniosité et leurs résultats diffèrent toutefois.
  - Ces attaques représentent environ **83 %** des attaques contre les chaînes d'approvisionnement des logiciels rendues publiques en 2023.
  - Les acteurs malveillants visent généralement des jetons compromis pour accéder à des infrastructures ou des services hébergés sur AWS, les plateformes Google ou GitHub.
  - Ce scénario peut être le prélude à une attaque de faible probabilité et aux conséquences importantes.
  - Les cybercriminels utilisent des techniques courantes telles que le typosquatting, le repojacking, la confusion de dépendance ou la compromission des comptes utilisateur pour obtenir un accès.

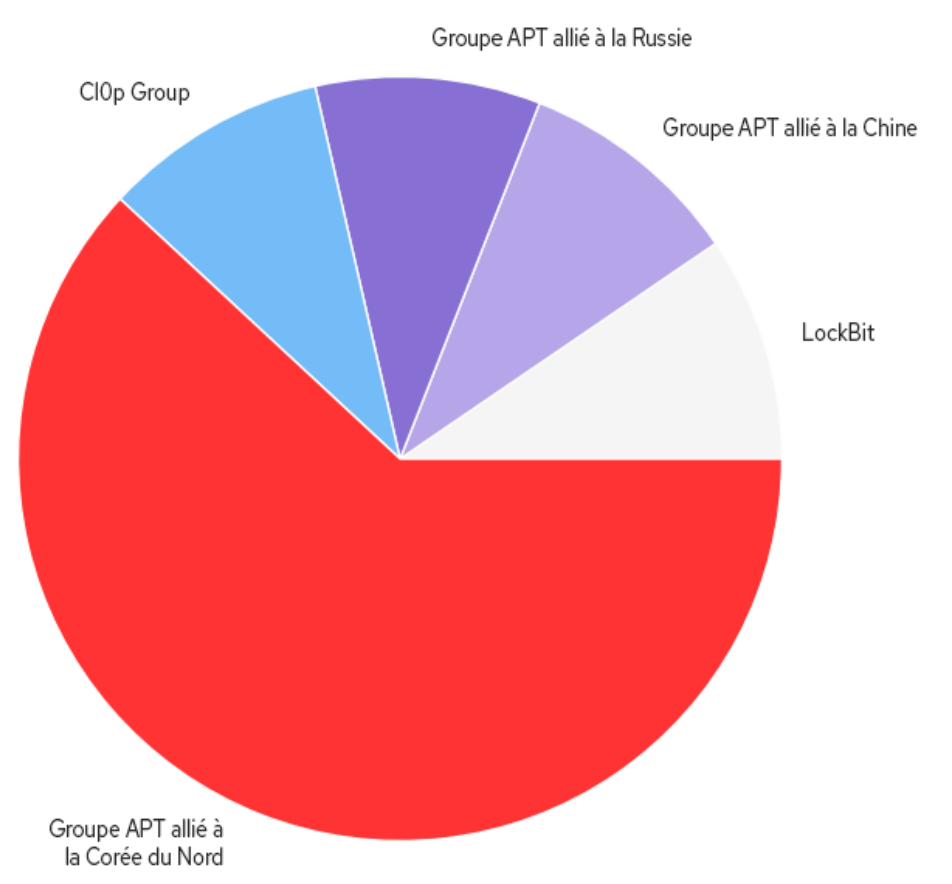


Figure 5 : cybercriminels connus à l'origine des attaques des chaînes d'approvisionnement des logiciels rendues publiques en 2023

D'après notre analyse des tendances entre 2022 et 2023, les secrets des développeurs de logiciels restent les éléments les plus convoités des cyberattaquants. La fuite de données secrètes est la technique la plus utilisée des deux côtés de la chaîne de cybersécurité. En voici des exemples :

- OSC&R (Open Software Supply Chain Attack Reference) : dans le cadre de la tactique ou de la phase d'impact de la chaîne de cyberattaque, la fuite de données secrètes est l'objectif ultime du cybercriminel. La faille très médiatisée du fournisseur de plateforme CI/CD CircleCI qui a provoqué en janvier 2023 la fuite de plusieurs secrets d'API en est la parfaite illustration.
- MITRE ATT&CK : une fuite de données secrètes peut permettre à un cybercriminel de passer à la phase d'accès initial, où il s'appliquera à compromettre la chaîne d'approvisionnement des logiciels. En contournant les phases de reconnaissance et de développement des ressources de la chaîne de cybersécurité, l'adversaire gagne du temps et économise des ressources.

Selon notre analyse, **81 %** des attaques contre les chaînes d'approvisionnement des logiciels en 2023 proviennent de l'utilisation abusive de plateformes Open Source populaires, telles que le gestionnaire de paquets npm et le référentiel PyPI (Python Package Index), le nombre de paquets malveillants détectés sur ces dernières ayant augmenté sensiblement. Les données accessibles au public montrent que les cybercriminels ciblent davantage la plateforme PyPI que npm.

Conclusion

Chez Red Hat, nous donnons la priorité à la gestion des risques pour nos clients. Cette année a été marquée par une forte augmentation des vulnérabilités de niveau Important (celles détectées, comme celles exploitées) et cette tendance va probablement se poursuivre. Il est donc crucial de nous concentrer sur les risques immédiats qui représentent le plus grand danger pour les clients et leurs déploiements s'ils sont exploités.

Une fois de plus, nous constatons que cette approche pragmatique produit des résultats alors que la majorité des vulnérabilités exploitées présentent toujours un niveau de gravité Critique ou Important. Notre capacité à nous adapter rapidement et à résoudre les vulnérabilités qui font l'objet d'une exploitation active en l'absence de correctifs illustre notre volonté d'atténuer des risques bien réels. L'application rapide de correctifs permet de protéger les clients des répercussions liées à l'exploitation des logiciels.

Il est très intéressant d'utiliser des données telles que la liste des CWE pour cibler des classes de vulnérabilités. Le recours à des langages sûrs pour la mémoire est lui aussi attirant, mais il pose d'autres problèmes. Comme nous l'avons constaté, si la protection de la mémoire n'aurait pas été bénéfique pour la majorité des vulnérabilités cette année (CWE-400), elle aurait cependant permis d'éviter les autres failles. L'utilisation de langages sûrs pour la mémoire lors de la rédaction d'un nouveau code est une bonne approche, qui présente toutefois moins d'intérêt pour la réécriture de codes bien rédigés et déployés depuis longtemps. À chaque modification de code, en particulier lorsque celui-ci est nouveau, les risques d'introduire de nouvelles vulnérabilités inconnues sont nombreux. Le flux de nouveaux logiciels pourrait par ailleurs augmenter davantage le nombre de vulnérabilités, du moins à court terme.

Enfin, il est déconcertant de constater que des attaques continues visent des chaînes d'approvisionnement Open Source. Grâce à son processus de sélection des logiciels et à l'utilisation de référentiels internes pour stocker le code utilisé, Red Hat se protège de ces attaques. En misant sur la stabilité et en minimisant les changements de code, nous évitons tout retour en amont de la chaîne qui nous exposerait à des attaques de point d'eau (« watering hole » en anglais). En optant pour une plateforme Open Source d'un éditeur tel que Red Hat, vous atténuez les effets de ces attaques contre les chaînes d'approvisionnement des logiciels.

Toutefois, il importe de garder à l'esprit que les logiciels Open Source ne proviennent pas toujours d'un fournisseur et qu'il faut veiller à maintenir des mécanismes de protection contre les attaques provenant directement de projets et de référentiels en amont.

Si utiliser un logiciel Red Hat permet de se prémunir contre ces types d'attaques, une protection efficace implique une responsabilité partagée. Les clients doivent savoir quels outils en amont ils utilisent et, dans tous les cas, être en mesure d'appliquer des correctifs plus rapidement pour protéger leurs ressources.

- Vincent Danen, vice-président Product Security, Red Hat

- Pour en savoir plus sur les processus de gestion des vulnérabilités que propose Red Hat, consultez le document Une approche ouverte de la gestion des vulnérabilités.
- Pour obtenir les dernières informations sur la sécurité des produits et services Red Hat, rendez-vous dans le Red Hat Product Security Center.

À propos de Red Hat

Premier éditeur mondial de solutions Open Source, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et automatiser des environnements complexes. Conseiller de confiance auprès des entreprises du Fortune 500, Red Hat propose des services d'assistance, de formation et de consulting reconnus qui apportent à tout secteur les avantages de l'innovation ouverte. Situé au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, Red Hat participe à la croissance et à la transformation des entreprises et les aide à se préparer à un avenir toujours plus numérique.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

Europe, Moyen-Orient et Afrique (EMEA)
00800 7334 2835
europe@redhat.com

France
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#1090925_0424