Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Secteur Transformation numérique et gouvernance de l'informatique (TNI)

18 octobre 2022

Programme de primes aux bogues eIAM

Rapport

Table des matières

1 Résumé

eIAM est le système central d’accès et d’autorisations de l’administration fédérale pour les applications web et les applications mobiles natives. Le secteur Transformation numérique et gouvernance de l’informatique (TNI) de la Chancellerie fédérale est responsable d’eIAM, dont l'exploitation incombe à l’Office fédéral de l’informatique et de la télécommunication (OFIT). Ces deux services ont travaillé avec le Centre national pour la cybersécurité (NCSC), responsable du programme de primes aux bogues (*bug bounty programme*), et la société Bug Bounty Switzerland SA pour organiser un programme privé de primes aux bogues qui s’est déroulé du 30 août au 11 octobre 2022.

Au total, 28 vulnérabilités ont été identifiées et signalées. 14 d’entre elles ont été reconnues comme valables. Des récompenses ont été versées aux pirates éthiques pour un montant final de 5 700 francs.

Le nombre de vulnérabilités signalées se situe dans la moyenne habituelle en cas de premier test avec des pirates éthiques. Du reste, aucune faille de sécurité critique n’a été trouvée.

Le programme de primes aux bogues eIAM a été suspendu pour que les organisateurs puissent évaluer les expériences réalisées et, si nécessaire, modifier certains aspects en vue d’éventuels nouveaux tests.

2 Contexte

eIAM est le système central d'accès et d'autorisations de l'administration fédérale pour les applications web et les applications mobiles natives. Il s'agit donc de l'infrastructure principale de gestion des accès de la Confédération. Il est utilisé par plus de 1000 applications spécialisées. L'infrastructure eIAM gère en moyenne 550 000 connexions par jour. Le secteur TNI est responsable du pilotage et de la gestion de l'infrastructure. L'OFIT en assure le développement et le fonctionnement.

Les programmes de primes aux bogues sont un moyen efficace et avantageux pour identifier les vulnérabilités d'un système. Aujourd'hui, les tests de sécurité standardisés ne suffisent souvent plus pour trouver les failles cachées. Le projet pilote mené au printemps 2021 dans l'administration fédérale a montré que les programmes de primes aux bogues permettaient d'identifier et de corriger efficacement les vulnérabilités des systèmes informatiques et des applications. Dès lors, la Confédération a décidé d'acquérir, en août 2022, une plateforme pour ce type de programmes[1].

Les programmes de primes aux bogues font appel au « piratage éthique », c'est-à-dire à des pirates informatiques qui recherchent des failles dans un cadre déterminé, pour détecter les vulnérabilités présentes dans les systèmes informatiques et les applications d'une organisation. Pour chaque bogue documentée et confirmée qu'il a découverte, le pirate reçoit une prime, dont le montant est fixé en fonction de la gravité de la faille, évaluée selon une norme internationale reconnue.

[1] L'administration fédérale fait l'acquisition d'une plateforme destinée aux programmes de primes aux bogues (admin.ch)

3 Réalisation

Le secteur TNI, responsable du service eIAM, l'OFIT, responsable de son exploitation, et le NCSC, responsable du programme de primes aux bogues, ont mené le projet en collaboration avec la société Bug Bounty Switzerland SA.

Le programme de primes aux bogues s'est déroulé du 30 août au 11 octobre 2022. Des pirates éthiques agréés ont été personnellement invités à y participer. Les opérations ont eu lieu dans l'environnement de test d'eIAM, dont la structure est identique à celle de l'environnement de production. Précisons que l'environnement de test ne contient que des données de test.

Au départ, il était prévu de prendre comme périmètre de test le système de gestion des comptes ainsi que diverses fonctionnalités de connexion (CH-Login, Harrods-Login, eIAM-Login et FED-Login). Après quatre semaines, ce périmètre a été étendu à d'autres fonctionnalités (gestion déléguée et KeyCloak OIDC).

Il a été décidé de ne collaborer qu'avec des pirates éthiques connus du NCSC ou de Bug Bounty Switzerland SA dont les compétences ont pu être constatées dans d'autres projets. Le nombre de pirates éthiques a été augmenté, de 9 à 32, au cours des deux premières semaines du programme.

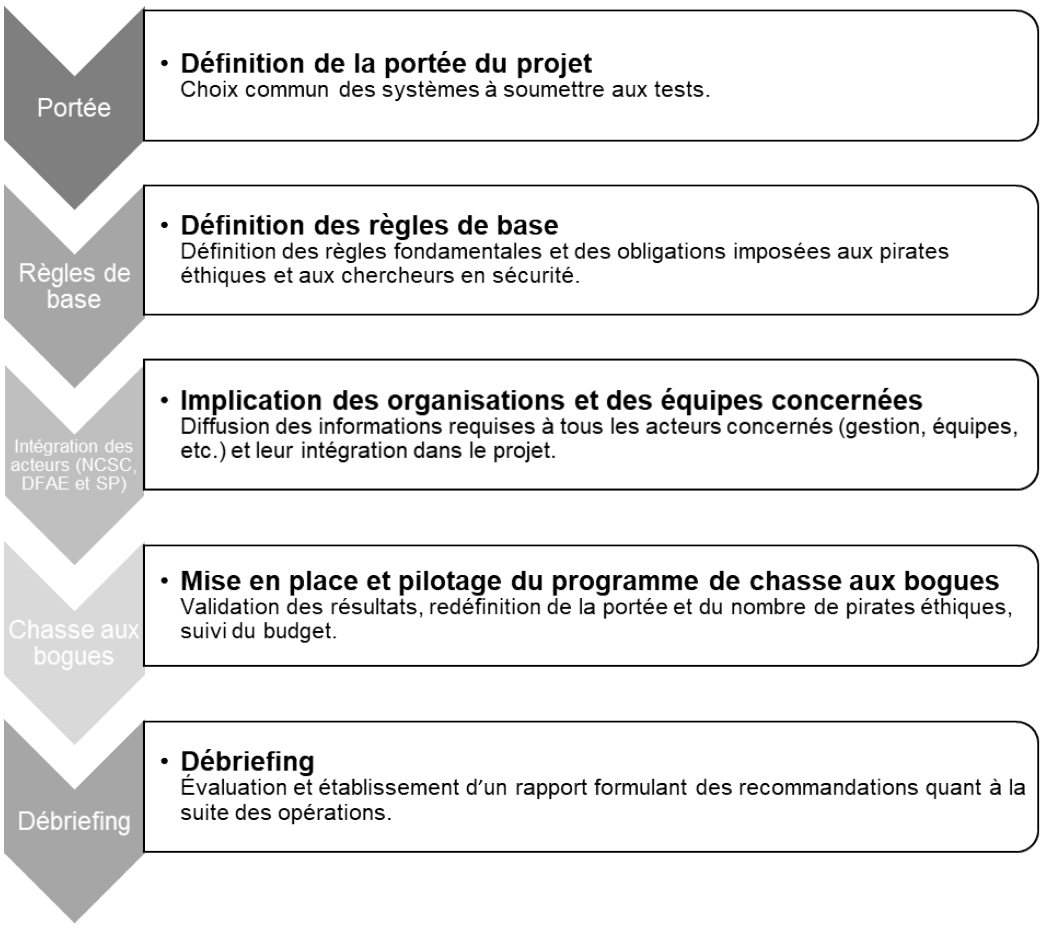
Les vulnérabilités ont été classées en fonction de leur criticité en tant que « faible », « moyen », « élevé » ou « critique », selon le système d'évaluation CVSS[2], utilisé dans le monde entier. Cette échelle permet aux services responsables et aux pirates éthiques de discuter de manière objective de la criticité et des conséquences des vulnérabilités. Les décalages entre criticité déclarée et criticité constatée ne sont pas inhabituels. Ils peuvent être expliqués par les paramètres utilisés par l'échelle.

L'équipe de développement d'eIAM a priorisé de la manière suivante la correction des vulnérabilités identifiées :

- critique : correction immédiate
- élevé : correction rapide
- moyen : correction à l'occasion des prochaines versions agendées
- faible : correction optionnelle, selon les conséquences potentielles

[2] Voir par ex. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Une procédure standard a été définie pour le programme de primes aux bogues de la Confédération. Son application a bien fonctionné :

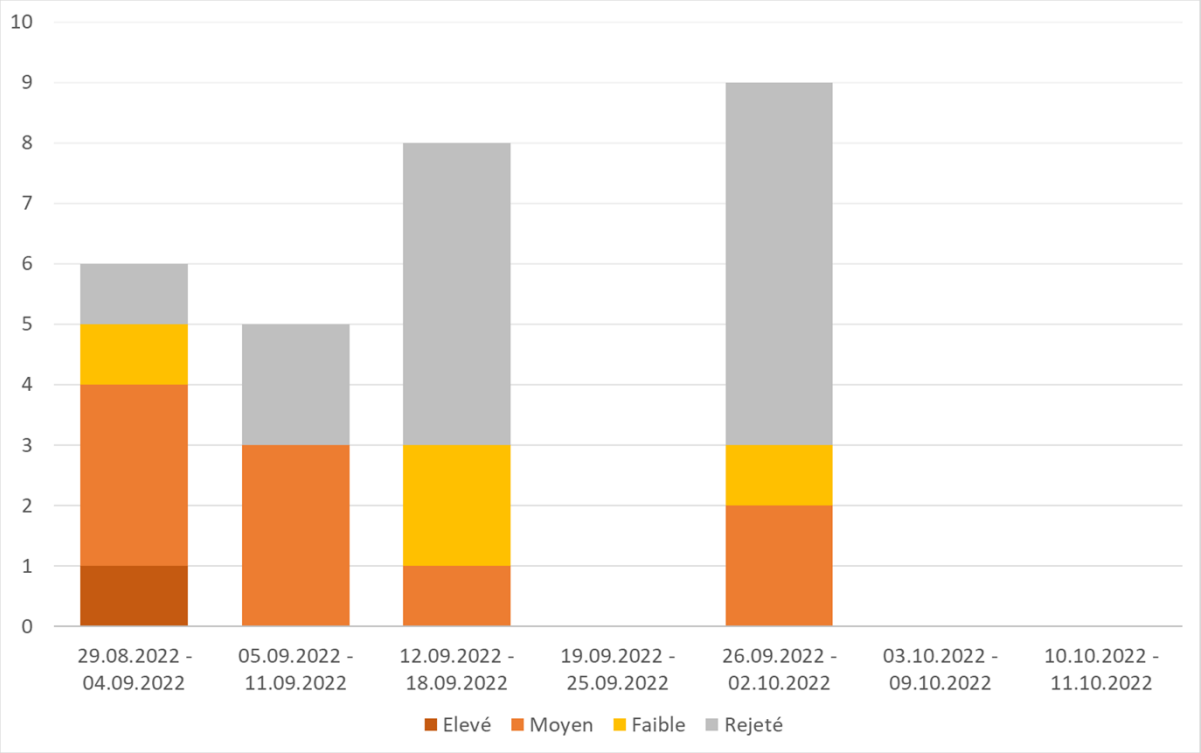


Le programme de primes aux bogues eIAM a été suspendu pour que les organisateurs puissent évaluer les expériences réalisées et, si nécessaire, modifier certains aspects en vue d'éventuels nouveaux tests.

4 Résultats

Entre le début du programme, le 30 août 2022 à 9 h, et sa fin provisoire, le 11 octobre 2022 à 23 h 59, 28 vulnérabilités ont été signalées. 14 d'entre elles ont été reconnues comme valables. Les autres vulnérabilités signalées n'ont pas été retenues parce qu'il s'agissait soit de doublons soit de cas n'entrant pas dans le périmètre de test prédéfini.

Le graphique suivant montre la répartition des signalements par semaine :



Les failles de sécurité confirmées se répartissent comme suit :

	Critique	Élevé	Moyen	Faible	Total
Nombre de vulnérabilités	**0**	**1**	**9**	**4**	**14**

La vulnérabilité de criticité « élevé » a pu être corrigée pendant le programme. Les autres seront corrigées à l'occasion des prochaines versions.

Le nombre important de signalements dans les premières semaines correspond à ce qui se passe habituellement lorsque des programmes de primes aux bogues sont lancés sur des périmètres de test nouveaux et que les pirates éthiques sont mus par une logique de compétition.

On a observé des interactions intéressantes entre les pirates et les services informatiques opérationnels responsables des systèmes et des applications. Grâce au très bon travail de documentation des pirates éthiques, les services responsables ont pu comprendre facilement les vulnérabilités et commencer aussitôt à les analyser. Ce genre de collaboration et de confiance sont déterminantes pour le bon déroulement des programmes de primes aux bogues.

5 Financement

La réalisation a été financée dans le cadre du budget de fonctionnement d’eIAM. Le total des primes versées s’élève à 5 700 francs.

6 Conclusion

Au cours des premières semaines du programme de primes aux bogues eIAM, il a pu être rapidement constaté que les vulnérabilités pouvaient être identifiées et traitées efficacement. La qualité et le contenu des signalements ont montré que cette méthode fonctionnait de manière complémentaire avec d’autres méthodes. En effet, les pirates éthiques identifient des vulnérabilités qui ne peuvent pas toujours être décelées lors des tests de sécurité habituels.