Backlog Courrier - Anomalie #28025

TMA - Analyse Vulnérabilité TinyMCE CVE-2023-45818 -> préconisation de mise à jour

21/02/2024 11:34 - Agnes GASTAMBIDE

Statut:	R&D - Terminé	**Début:**	21/02/2024
Priorité:	1-Majeur	**Echéance:**	29/02/2024
Assigné à:	Hamza HRAMCHI		
Catégorie:			
Version cible:	21.03 TMA8		
Version applicable MC:	21.03 TMA	**Tags Courrier:**	

Description

L'éditeur de texte JavaScript TinyMCE est déployé dans une version vulnérable (5.10.7) à la CVE-2023-45818.
Pouvez-vous nous faire un retour sur votre analyse et vos préconisations sur le sujet.

Merci.

Historique

#3 - 21/02/2024 11:38 - Emmanuel DILLARD

- Sujet changé de TMA - 21.03 - Analyse Vulnérabilité TinyMCE à TMA - Analyse Vulnérabilité TinyMCE CVE-2023-45818

- Echéance mis à 26/02/2024

- Statut changé de A qualifier à R&D - A étudier

- Version applicable MC mis à 21.03 TMA

https://www.cve.org/CVERecord?id=CVE-2023-45818

#4 - 26/02/2024 12:02 - Emmanuel DILLARD

- Sujet changé de TMA - Analyse Vulnérabilité TinyMCE CVE-2023-45818 à TMA - Analyse Vulnérabilité TinyMCE CVE-2023-45818 -> préconisation de mise à jour

- Echéance 26/02/2024 supprimé

- Statut changé de R&D - A étudier à R&D - A planifier

- Priorité changé de 2-Sérieux à 1-Majeur

#5 - 27/02/2024 12:42 - Emmanuel DILLARD

- Statut changé de R&D - A planifier à R&D - En cours

- Assigné à Emmanuel DILLARD supprimé

#6 - 27/02/2024 15:13 - Emmanuel DILLARD

- Echéance mis à 29/02/2024

#8 - 29/02/2024 14:37 - Hamza HRAMCHI

- Assigné à mis à Hamza HRAMCHI

#9 - 29/02/2024 14:55 - Hamza HRAMCHI

- **Nom de la vulnérabilité** : Mutation Cross-Site Scripting (mXSS) dans TinyMCE.
- **Description** :
  La vulnérabilité de mutation Cross-Site Scripting (mXSS) dans TinyMCE concerne la manière dont TinyMCE gère les opérations d'annulation et de rétablissement des modifications apportées au contenu édité dans l'éditeur. Lorsqu'un utilisateur effectue des modifications dans l'éditeur

TinyMCE, ces modifications sont enregistrées dans une pile d'annulation qui permet à l'utilisateur d'annuler ces modifications et de les rétablir ultérieurement.
Cependant, dans certaines circonstances, si du code HTML malveillant est inséré dans le contenu édité et que ce contenu passe avec succès la désinfection contre les attaques de type Cross-Site Scripting (XSS), il peut être manipulé de manière incorrecte lors de son stockage dans la pile d'annulation. Cette manipulation incorrecte peut découler de l'utilisation de fonctions de manipulation de chaînes internes.
Lorsque le contenu HTML est ensuite récupéré à partir de la pile d'annulation et rétabli, il est soumis à une analyse supplémentaire par le navigateur à l'aide de l'API DOMParser native ou de l'API SaxParser (selon la version de TinyMCE). Cette analyse peut entraîner une mutation malveillante de l'HTML, permettant l'exécution de charges utiles XSS.
En résumé, cette vulnérabilité permet à un attaquant de faire exécuter du code JavaScript malveillant dans le contexte du navigateur de l'utilisateur en exploitant des opérations d'annulation et de rétablissement dans TinyMCE.

- **Versions affectées** : TinyMCE 5 jusqu'à la version 5.10.7.
- **Correctif** : La vulnérabilité a été corrigée à partir de TinyMCE 5.10.8 en s'assurant que l'HTML est supprimé en utilisant une manipulation au niveau des nœuds plutôt qu'une manipulation de chaîne.
- **Conseil de sécurité** : Mise à niveau vers les versions corrigées (recommandé : dernière version : 6.8.3).
- **Solutions de contournement** : Aucune solution de contournement n'est connue pour cette vulnérabilité.
- **Risques associés** : L'exploitation de cette vulnérabilité peut entraîner l'exécution de scripts malveillants dans le contexte du navigateur de l'utilisateur, ce qui peut conduire à des attaques de type Cross-Site Scripting (XSS) et à la compromission des données utilisateur.

#10 - 29/02/2024 14:55 - Hamza HRAMCHI

- Statut changé de R&D - En cours à R&D - En test

#13 - 05/03/2024 15:24 - Joseph AKEL

- Statut changé de R&D - En test à R&D - Terminé

Fichiers

tinymce.jpg	35,9 ko	21/02/2024	Agnes GASTAMBIDE