ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Supply chain attaque cible deux Actions populaires de GitHub
Numéro de Référence	53532703 /25
Date de Publication	27 Mars 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- GitHub Action : tj-actions/changed-files version antérieure à v46.0.1.
- GitHub Action : reviewdog/action-setup version antérieure à reviewdog/action-setup@3f401fe.

Identificateurs externes

- CVE-2025-30066, CVE-2025-30154

Bilan de la vulnérabilité

Deux Actions populaires de GitHub (tj-actions/changed-files et reviewdog/action-setup) ont été compromises. La compromission de la chaîne d'approvisionnement permet à des attaquants d'accéder à des secrets sensibles dans des projets utilisant ces Actions. Les secrets potentiellement exposés incluent (Clés d'accès valides, Tokens d'accès personnel GitHub (PATs), Tokens npm et Clés RSA privées).

- La vulnérabilité « CVE-2025-30066 » affecte toutes les versions de l'Action GitHub tj-actions/changed-files exécutées entre le 12 mars 2025 à 01:00 (GMT+1) et le 15 mars 2025 à 13:00 (GMT+1). Cette action a été compromise pour intégrer un script Python malveillant qui extrait des secrets (clés d'accès, jetons d'authentification, etc.) depuis la mémoire du processus Runner Worker et les expose dans les logs GitHub.

- La vulnérabilité « CVE-2025-30154 » concerne toutes les versions de l'action « reviewdog/action-setup » exécutées entre le 11 mars 2025 (19:42 (GMT+1)) et le 11 mars 2025 (21:31 (GMT+1)). Cette faille a potentiellement permis aux attaquants de compromettre d'autres Actions associées à reviewdog, entraînant des risques similaires de divulgation de secrets.

Solution :

Veuillez se référer aux bulletins de sécurité GitHub pour plus d'information.

Il est recommandé de prendre les mesures suivantes :

- Effectuer un audit pour localiser tous les projets utilisant tj-actions/changed-files ou reviewdog/action-setup dans les plages horaires et versions compromises.
- Vérifier les workflows ayant exécuté des commits malveillants pour identifier les secrets potentiellement compromis.
- Remplacer immédiatement les clés d'accès, tokens GitHub, tokens npm, et clés RSA privées exposés.
- Mettre à jour tj-actions/changed-files vers v46.0.1.
- Mettre à jour reviewdog/action-setup vers la version corrigée reviewdog/action-setup@3f401fe.

Risque :

- Divulgation des informations sensibles
- Compromission des systèmes
- Exécution de code malveillant

Indicateurs de compromission (IoC) :

Malicious commit:

- 0e58ed8671d6b60d0890c21b07f8835ace038e67

Annexe

Bulletin de sécurité GitHub du 25 mars 2025**:**

- https://github.com/advisories/GHSA-mrrh-fwg8-r2c3

Bulletin de sécurité CISA du 26 mars 2025**:**

- https://www.cisa.gov/news-events/alerts/2025/03/18/supply-chain-compromise-third-party-tj-actionschanged-files-cve-2025-30066-and-reviewdogaction