AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Deux failles critiques permettent une prise de contrôle à distance sur n8n

Contenu

I. Contexte

La plateforme d'automatisation de workflows n8n, largement utilisée pour l'intégration d'APIs et de services d'IA, est actuellement soumise à deux failles de vulnérabilités critiques. Découvertes par des chercheurs en cybersécurité, elles permettent de briser l'isolement du code (sandbox) pour obtenir une exécution de code arbitraire (RCE) sur l'hôte.

Bien que n8n soit un outil puissant pour l'automatisation de tâches complexes, ces failles rappellent la difficulté intrinsèque de sécuriser l'exécution de langages dynamiques comme JavaScript et Python.

II. Détails Techniques des Vulnérabilités

Les failles exploitent des mécanismes subtils des langages de programmation pour contourner les listes d'interdiction (deny lists) et les contrôles basés sur l'Arbre de Syntaxe Abstraite (AST).

CVE-2026-1470 : Évasion de la Sandbox JavaScript (Score CVSS : 9.9)

Malgré la nécessité d'une authentification, cette faille est jugée critique car elle touche le nœud principal de n8n.

- Mécanisme : Une mauvaise manipulation de l'instruction with en JavaScript permet à un identifiant de constructeur autonome de contourner la désinfection des données.
- Impact : L'attaquant peut résoudre l'identifiant vers la fonction Function, permettant l'exécution de JavaScript arbitraire et une prise de contrôle totale (RCE) de l'instance.

CVE-2026-0863 : Évasion de la Sandbox Python

Cette vulnérabilité cible les workflows utilisant Python comme sous-processus.

- Mécanisme : Elle combine l'introspection d'objets via les chaînes de formatage (format-strings) avec un comportement spécifique des erreurs (AttributeError.obj) dans Python 3.10+.
- Impact : Ce chaînage permet de regagner l'accès aux fonctions natives (builtins) et aux imports restreints, autorisant l'exécution de commandes système.

III. Analyse du Risque et Contexte

L'exploitation de la CVE-2026-1470 nécessite des privilèges permettant de créer ou modifier un workflow. Cependant, elle est classée Critique car elle permet à un utilisateur

simple (non-administrateur) de s'extraire de sa cage logicielle pour pivoter vers un contrôle total de l'infrastructure.

Le contexte est d'autant plus tendu que la plateforme a récemment été frappée par la faille "Ni8mare", une vulnérabilité d'une sévérité maximale permettant une prise de contrôle sans authentification. Les données récentes montrent une lenteur inquiétante dans l'application des correctifs :

- Début janvier : 60 000 instances vulnérables à "Ni8mare".
- Fin janvier : 39 900 instances toujours exposées.

IV. Mesures de Remédiation

Il est impératif pour les administrateurs d'instances auto-hébergées de mettre à jour leurs environnements immédiatement. Les versions cloud de n8n ont déjà été sécurisées par l'éditeur.

Vulnérabilité	Versions Correctives
CVE-2026-1470	1.123.17, 2.4.5, 2.5.1
CVE-2026-0863	1.123.14, 2.3.5, 2.4.2

V. Conclusion

Néanmoins, pour éviter d'être victime d'un acteur malveillant connu ou non, il est recommandé de prendre les précautions suivantes :

- N'installer que les applications qui vous sont utiles ;
- Se rassurer de la crédibilité d'une application à l'aide des notes et commentaires attribués par les utilisateurs à celle-ci, avant de les installer ;
- Installer les applications depuis le Store officiel de votre Système d'exploitation (Play Store pour Google Android, App Store pour IOS, etc.) ;
- N'accordez que les autorisations utiles à vos applications pour réaliser les fonctions qu'elles sont censées réaliser ;
- Veillez à mettre à jour régulièrement tous vos logiciels, en installant chaque nouveau correctif de sécurité dès sa publication ;

- Choisissez une solution de sécurité (Antivirus) éprouvée dotée de capacités de détection comportementale pour une protection efficace contre les menaces connues et inconnues, notamment les exploitations de vulnérabilités ;
- Armez-vous des règles élémentaires de cyber-hygiène.