aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans Node.js

2024-01-23 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Node.JS - CVE-2023-39332

Publié le 13 octobre 2023 sur le site de l'éditeur, la CVE-2023-39332 est une vulnérabilité critique affectant *Node.js*.

Le chercheur en sécurité Tobias Nießen a identifié une restriction incorrecte à l'accès aux répertoires (*Path Traversal*) lors du traitement d'objets *Uint8Array* qui ne sont pas de type *Buffer*.

Il est ainsi possible pour un attaquant distant et non authentifié, en utilisant des requêtes forgées, de contourner des mesures de sécurité et d'accéder à des espaces mémoires non authorisés.

Depuis le 20 janvier 2024, une preuve de concept est disponible en sources ouvertes.

Risques

- Contournement de la politique de sécurité

Type de vulnérabilité

- *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Preuve de concept

Une preuve de concept est disponible depuis le 20 janvier 2024.

Produits impactés

- Node.js versions 18.x antérieures à 18.18.2
- Node.js versions 20.x antérieures à 20.8.1

Produits dépendants

- IBM Answer Retrieval for Watson Discovery 2.7.0
- IBM Business Automation Workflow Enterprise Service Bus 22.0.2
- IBM Business Automation Workflow Enterprise Service Bus 23.0.1
- IBM Business Automation Workflow traditional 19.0.0.1
- IBM Business Automation Workflow traditional 19.0.0.3

- IBM Business Automation Workflow traditional 20.0.0.1
- IBM Business Automation Workflow traditional 20.0.0.2
- IBM Business Automation Workflow traditional 21.0.1
- IBM Business Automation Workflow traditional 21.0.3.1
- IBM Business Automation Workflow traditional 22.0.1
- IBM Business Automation Workflow traditional 22.0.2
- IBM Business Automation Workflow traditional 23.0.1
- IBM Cloud Transformation Advisor 2.0.1
- IBM Cloud Transformation Advisor 3.7.1
- IBM Spectrum Control 5.4
- Fedora

Recommandations

Node JS

- Appliquer la dernière version de *Node.js* disponible ici.
- Des informations complémentaires sont disponibles sur le site de l'éditeur.

IBM

- Pour *IBM Answer Retrieval for Watson Discovery*, mettre à jour vers la version 2.15.0 ou ultérieure (Correctif disponible ici)
- Pour *IBM Spectrum Control*, mettre à jour vers la version 5.4.11 ou ultérieure (Correctif disponible ici)
- Pour *IBM Business Automation Workflow traditional*, appliquer le correctif DT245355
- Pour *IBM Business Automation Workflow Enterprise Service Bus*, appliquer le correctif DT245355.
- Des informations complémentaires pour *IBM Business Automation Workflow* sont disponibles ici.
- Des informations complémentaires pour *IBM Spectrum Control* sont disponible ici.
- Des informations complémentaires pour *IBM Answer Retrieval for Watson Discovery* ici.

Fedora

- Appliquer la dernière mise à jour de *Fedora*.
- Des informations complémentaires sont disponibles sur le site de l'éditeur.

Références

- https://nvd.nist.gov/vuln/detail/CVE-2023-39332
- https://security.netapp.com/advisory/ntap-20231116-0009/
- https://exchange.xforce.ibmcloud.com/vulnerabilities/268788
- https://nodejs.org/en/blog/vulnerability/october-2023-security-releases
- https://bodhi.fedoraproject.org/updates/FEDORA-2023-4d2fd884ea
- https://www.ibm.com/support/pages/node/7087510?_ga=2.199109674.424467990.1705926133-1391590523.1663137482
- https://www.ibm.com/support/pages/node/7108595?_ga=2.199109674.424467990.1705926133-1391590523.1663137482
- https://www.ibm.com/support/pages/node/7109016?_ga=2.199803307.424467990.1705926133-1391590523.1663137482