



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits IBM
Numéro de Référence	40801403/23
Date de Publication	14 Mars 2023
Risque	Important
Impact	Important

Systèmes affectés

- IBM QRadar WinCollect Agent versions 10.x antérieures à 10.1.3
- IBM Cognos Analytics versions 11.2.x antérieures à 11.2.3
- IBM Cognos Analytics versions 11.1.x antérieures à 11.1.7 avec le dernier correctif de sécurité (Fix Pack 6)

Identificateurs externes

- CVE-2020-4051 , CVE-2021-29425 , CVE-2021-3711 , CVE-2021-3712 , CVE-2021-3733 , CVE-2021-3737 , CVE-2021-4160 , CVE-2021-43138 , CVE-2022-0391 , CVE-2022-24758 , CVE-2022-25881 , CVE-2022-34339 , CVE-2022-4203 , CVE-2022-4304 , CVE-2022-43879 , CVE-2022-4450 , CVE-2023-0215 , CVE-2023-0216 , CVE-2023-0217 , CVE-2023-0286 , CVE-2023-0401 , CVE-2023-23914 , CVE-2023-23915 , CVE-2023-23916

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits IBM susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant de porter atteinte à la confidentialité des données, de contourner la politique de sécurité, de causer un déni de service à distance et de réussir une exécution de code arbitraire à distance.

Solution

Veuillez se référer au bulletin de sécurité IBM du 10 Mars 2023 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Déni de service
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité IBM du 10 Mars 2023:

- <https://www.ibm.com/support/pages/node/6962773>
- <https://www.ibm.com/support/pages/node/6962775>