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	Vulnérabilités dans les produits IBM
Numéro de Référence	42381206/23
Date de Publication	12 Juin 2023
Risque	Important
Impact	Important

Systèmes affectés

- IBM WebSphere Service Registry and Repository versions 8.5.x antérieures sans le dernier correctif de sécurité V8.5.6.3_IJ47124
- IBM WebSphere Service Registry and Repository Studio versions 8.5.x sans le dernier correctif de sécurité V8.5.6.3_IJ47124
- QRadar WinCollect Agent versions 10.0.x à 10.1.x antérieures à 10.1.4
- IBM QRadar User Behavior Analytics versions 1.x à 4.1.x antérieures à 4.1.12
- IBM QRadar Deployment Intelligence App versions 2.x à 3.0.x antérieures à 3.0.10
- IBM MaaS360 Cloud Extender Agent versions antérieures à 3.000.100.069
- IBM MaaS360 Cloud Extender Base Module versions antérieures à 3.000.100.069
- IBM MaaS360 Configuration Utility versions antérieures à 3.000.100
- IBM MaaS360 PKI Certificate Module versions antérieures à 3.000.100
- IBM MaaS360 Mobile Enterprise Gateway versions antérieures à 3.000.100
- IBM MaaS360 VPN versions antérieures à 3.000.100
- IBM Sterling Partner Engagement Manager Essentials Edition versions 6.1.2.x antérieures à 6.1.2.8
- IBM Sterling Partner Engagement Manager Standard Edition versions 6.1.2.x antérieures à 6.1.2.8
- IBM Sterling Partner Engagement Manager Essentials Edition versions 6.2.0.x antérieures à 6.2.0.6
- IBM Sterling Partner Engagement Manager Standard Edition versions 6.2.0.x antérieures à 6.2.0.6

- IBM Sterling Partner Engagement Manager Essentials Edition versions 6.2.1.x antérieures à 6.2.1.3
- IBM Sterling Partner Engagement Manager Standard Edition versions 6.2.1.x antérieures à 6.2.1.3
- IBM Sterling Partner Engagement Manager Essentials Edition versions 6.2.2.x antérieures à 6.2.2.1
- IBM Sterling Partner Engagement Manager Standard Edition versions 6.2.2.x antérieures à 6.2.2.1

Identificateurs externes

- CVE-2022-3171 , CVE-2022-41881 , CVE-2022-40152 , CVE-2022-31160 , CVE-2017-7525 , CVE-2022-25168 , CVE-2022-3509 , CVE-2022-41854 , CVE-2022-38752 , CVE-2022-1471 , CVE-2021-37533 , CVE-2022-42004 , CVE-2022-42003 , CVE-2022-41915 , CVE-2022-4450 , CVE-2023-0216 , CVE-2023-0401 , CVE-2022-4203 , CVE-2023-0217 , CVE-2023-27536 , CVE-2023-27533 , CVE-2023-27537 , CVE-2023-27534 , CVE-2023-27538 , CVE-2023-27535 , CVE-2022-4304 , CVE-2023-0215 , CVE-2023-0286 , CVE-2022-25881 , CVE-2021-23440 , CVE-2022-24785 , CVE-2022-46175 , CVE-2023-29257 , CVE-2023-29255 , CVE-2023-27555 , CVE-2023-26021 , CVE-2023-25930 , CVE-2023-26022 , CVE-2023-27559 , CVE-2023-23916 , CVE-2023-24998, CVE-2023-21930 , CVE-2023-21937 , CVE-2023-21938 , CVE-2023-21954 , CVE-2023-21967 , CVE-2023-21968 , CVE-2023-27533 , CVE-2023-27534 , CVE-2023-27535 , CVE-2023-27536 , CVE-2023-27537 , CVE-2023-27538

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 contourner la politique de sécurité, de causer un déni de service à distance et d'exécuter du code arbitraire à distance.

Solution

Veuillez se référer au bulletin de sécurité IBM pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Déni de service
- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité IBM:

- https://www.ibm.com/support/pages/node/7002387
- https://www.ibm.com/support/pages/node/7002501