

Agence Nationale  
des Systèmes d'information  
de l'état

Djibouti le, 11-02-2024

## **BULLETIN ALERTES**

Object	Multiples vulnérabilités dans les produits IBM
Référence	1105
Date de Publication	2024-02-11
Sévérité	Critique

### **IMPACT :**

- Exécution de code arbitraire à distance
- Déni de service à distance
- Contournement de la politique de sécurité
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Élévation de privilèges
- Injection de code indirecte à distance (XSS)

### **SYSTÈME AFFECTÉ :**

- QRadar Pulse App versions antérieures à 2.2.12
- MaaS360 Cloud Extender Agent versions antérieures à 3.000.300.025?
- MaaS360 Mobile Enterprise Gateway versions antérieures à 3.000.400?
- MaaS360 VPN versions antérieures à 3.000.400
- Sterling Control Center versions antérieures à 6.3.0.0 iFix04
- Sterling B2B Integrator version 6.0.x antérieures à 6.0.3.9
- Sterling B2B Integrator version 6.1.x antérieures à 6.1.2.4
- Sterling File Gateway version 6.0.x antérieures à 6.0.3.9
- Sterling File Gateway version 6.1.x antérieures à 6.1.2.4
- Sterling Transformation Extender versions 10.1.0, 10.1.1, 10.1.2 et 11.0.0 sans le correctif de sécurité APAR PH58718

## DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans les produits IBM. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et un déni de service à distance.

## SOLUTION :

- METTRE À JOUR les produits IBM.
- Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## DOCUMENTATION :

- Bulletin de sécurité IBM :

<https://www.ibm.com/support/pages/node/7114777>

- CVE-2010-3300

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3300>

- CVE-2016-100027

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-100027>

- CVE-2022-25883

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25883>

- CVE-2022-40609

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40609>

- CVE-2023-20883

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20883>

- CVE-2023-22067

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22067>

- CVE-2023-22081

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22081>

- CVE-2023-32002

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32002>

- CVE-2023-32006

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32006>

- CVE-2023-34149

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34149>

- CVE-2023-34396  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34396>
- CVE-2023-4807  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4807>
- CVE-2023-5363  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5363>
- CVE-2023-34453  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34453>
- CVE-2023-34454  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34454>
- CVE-2023-34455  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34455>
- CVE-2023-34462  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-34462>
- CVE-2023-36478  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36478>
- CVE-2023-36479  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36479>
- CVE-2023-40167  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40167>
- CVE-2023-41900  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41900>
- CVE-2023-44487  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487>
- CVE-2023-46308  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46308>
- CVE-2023-46849  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46849>
- CVE-2023-46850  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46850>
- CVE-2023-5676  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5676>