

Agence Nationale  
des Systèmes d'information  
de l'état

Djibouti le, 09-09-2024

## **BULLETIN ALERTES**

Object	Multiples vulnérabilités dans les produits IBM
Référence	1242
Date de Publication	2024-09-09
Sévérité	Critique

### **IMPACT :**

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

### **SYSTÈME AFFECTÉ :**

- Cloud Pak versions 1.10.x.x antérieures à 1.10.25.0
- QRadar Assistant version antérieures à 3.8.0
- QRadar Suite Software versions 1.10.x.x postérieures à 1.10.12.x et antérieures à 1.10.25.0
- Security QRadar EDR version 3.12.x antérieures à 3.12.11
- Sterling Control Center version 6.2.1.x antérieures à 6.2.1.0 iFix13
- Tivoli Monitoring version 6.3.x antérieures à 6.3.0.7 Plus Service Pack 5

## DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans les produits IBM. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données.

## SOLUTION :

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## DOCUMENTATION :

- Bulletin de sécurité IBM 7167122 du 03 septembre 2024

<https://www.ibm.com/support/pages/node/7167122>

- Bulletin de sécurité IBM 7167218 du 04 septembre 2024

<https://www.ibm.com/support/pages/node/7167218>

- Bulletin de sécurité IBM 7166853 du 05 septembre 2024

<https://www.ibm.com/support/pages/node/7166853>

- Bulletin de sécurité IBM 7167599 du 05 septembre 2024

<https://www.ibm.com/support/pages/node/7167599>

- Bulletin de sécurité IBM 7167607 du 05 septembre 2024

<https://www.ibm.com/support/pages/node/7167607>

- CVE-2021-23727

<https://www.cve.org/CVERecord?id=CVE-2021-23727>

- CVE-2022-41678
- <https://www.cve.org/CVERecord?id=CVE-2022-41678>
- CVE-2024-34069

<https://www.cve.org/CVERecord?id=CVE-2024-34069>

- CVE-2024-35153

<https://www.cve.org/CVERecord?id=CVE-2024-35153>

- CVE-2024-35154

<https://www.cve.org/CVERecord?id=CVE-2024-35154>

- CVE-2024-35195

<https://www.cve.org/CVERecord?id=CVE-2024-35195>

- CVE-2024-37532

<https://www.cve.org/CVERecord?id=CVE-2024-37532>

- CVE-2024-37890

<https://www.cve.org/CVERecord?id=CVE-2024-37890>

- CVE-2024-37891

<https://www.cve.org/CVERecord?id=CVE-2024-37891>

- CVE-2024-38472

<https://www.cve.org/CVERecord?id=CVE-2024-38472>

- CVE-2024-38473

<https://www.cve.org/CVERecord?id=CVE-2024-38473>

- CVE-2024-38474

<https://www.cve.org/CVERecord?id=CVE-2024-38474>

- CVE-2024-38475

<https://www.cve.org/CVERecord?id=CVE-2024-38475>

- CVE-2024-38476

<https://www.cve.org/CVERecord?id=CVE-2024-38476>

- CVE-2024-38477

<https://www.cve.org/CVERecord?id=CVE-2024-38477>

- CVE-2024-39338

<https://www.cve.org/CVERecord?id=CVE-2024-39338>

- CVE-2024-39573

<https://www.cve.org/CVERecord?id=CVE-2024-39573>

- CVE-2024-39689

<https://www.cve.org/CVERecord?id=CVE-2024-39689>

- CVE-2024-39705

<https://www.cve.org/CVERecord?id=CVE-2024-39705>

- CVE-2024-39884

<https://www.cve.org/CVERecord?id=CVE-2024-39884>

- CVE-2024-4068

<https://www.cve.org/CVERecord?id=CVE-2024-4068>

- CVE-2024-40725

<https://www.cve.org/CVERecord?id=CVE-2024-40725>

- CVE-2024-40898

<https://www.cve.org/CVERecord?id=CVE-2024-40898>

- CVE-2024-41110

<https://www.cve.org/CVERecord?id=CVE-2024-41110>

- CVE-2024-6345

<https://www.cve.org/CVERecord?id=CVE-2024-6345>

- CVE-2024-6387

<https://www.cve.org/CVERecord?id=CVE-2024-6387>