

Agence Nationale  
des Systèmes d'information  
de l'état

Djibouti le, 04-02-2024

## **BULLETIN ALERTES**

Object	Multiplés Vulnérabilités dans Juniper
Référence	1102
Date de Publication	2024-02-01
Sévérité	Critique

### **IMPACT :**

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

### **SYSTÈME AFFECTÉ :**

- Secure Analytics versions antérieures à 7.5.0 UP7
- Secure Analytics - Log Collector versions antérieures à v1.8.4
- Secure Analytics - SOAR Plugin App versions antérieures à 5.3.1
- Secure Analytics - Deployment Intelligence App versions antérieures à 3.0.12
- Secure Analytics - User Behavior Analytics Application add-on versions antérieures à 4.1.14

### **DÉSCRIPTION :**

Des nombreuses vulnérabilités ont été découvertes dans les produits Juniper susmentionné.

Ces vulnérabilités permettent à un attaquant distant d'exécuter du code arbitraire, un déni de service à distance et un contournement de la politique de sécurité.

## SOLUTION :

Mettre à jour vos produits Juniper. (se réfère à la documentation)

## DOCUMENTATION :

- Bulletin de sécurité Juniper 01/02/2024  
[https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Serie-s-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en\\_US](https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Serie-s-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US)
- CVE-2023-35116  
<https://www.cve.org/CVERecord?id=CVE-2023-35116>
- CVE-2023-34453  
<https://www.cve.org/CVERecord?id=CVE-2023-34453>
- CVE-2023-34455  
<https://www.cve.org/CVERecord?id=CVE-2023-34455>
- CVE-2023-34454  
<https://www.cve.org/CVERecord?id=CVE-2023-34454>
- CVE-2023-43642  
<https://www.cve.org/CVERecord?id=CVE-2023-43642>
- CVE-2023-2976  
<https://www.cve.org/CVERecord?id=CVE-2023-2976>
- CVE-2023-33201  
<https://www.cve.org/CVERecord?id=CVE-2023-33201>
- CVE-2023-46136  
<https://www.cve.org/CVERecord?id=CVE-2023-46136>
- CVE-2023-43804  
<https://www.cve.org/CVERecord?id=CVE-2023-43804>
- CVE-2023-37920  
<https://www.cve.org/CVERecord?id=CVE-2023-37920>
- CVE-2022-25883  
<https://www.cve.org/CVERecord?id=CVE-2022-25883>
- CVE-2023-45133  
<https://www.cve.org/CVERecord?id=CVE-2023-45133>
- CVE-2023-31484  
<https://www.cve.org/CVERecord?id=CVE-2023-31484>
- CVE-2023-1370  
<https://www.cve.org/CVERecord?id=CVE-2023-1370>
- CVE-2021-4048  
<https://www.cve.org/CVERecord?id=CVE-2021-4048>
- CVE-2021-23445  
<https://www.cve.org/CVERecord?id=CVE-2021-23445>
- CVE-2021-31684  
<https://www.cve.org/CVERecord?id=CVE-2021-31684>
- CVE-2023-38019  
<https://www.cve.org/CVERecord?id=CVE-2023-38019>
- CVE-2023-38020  
<https://www.cve.org/CVERecord?id=CVE-2023-38020>
- CVE-2023-38263  
<https://www.cve.org/CVERecord?id=CVE-2023-38263>

- CVE-2024-21611  
<https://www.cve.org/CVERecord?id=CVE-2024-21611>
- CVE-2022-3171  
<https://www.cve.org/CVERecord?id=CVE-2022-3171>
- CVE-2022-3509  
<https://www.cve.org/CVERecord?id=CVE-2022-3509>
- CVE-2024-21611  
<https://www.cve.org/CVERecord?id=CVE-2024-21611>