



**DJ-CERT**

Centre national de veille,  
d'alerte et de réponse aux  
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 07-02-2023

## **BULLETIN ALERTES**

Objet	Vulnérabilité dans Cisco IOx
Référence	1028
Date de Publication	2023-02-07
Sévérité	Elevé

### **IMPACT :**

- Exécution de code arbitraire à distance

### **SYSTÈME AFFECTÉ :**

- Routeurs industriels Cisco séries 800 versions antérieures à 15.9(3)M7
- AP Catalysts (COS-APs) versions antérieures à 17.3.8, 17.9.2 et 17.11.1
- CGR1000 Compute Modules
- IC3000 Industrial Compute Gateways versions antérieures à 1.2.1
- IOS XE versions antérieures à 17.6.5, 17.9.2 et 17.10.1
- Routeurs industriels IR510 WPAN

### **DÉSCRIPTION :**

Une vulnérabilité a été découverte dans les produits Cisco IOx susmentionné .Elle permet à un attaquant distant d'exécuter du code arbitraire à distance.

### **SOLUTION :**

Mettre à jour vos Cisco IOx.(se référer à la documentation)

**DOCUMENTATION :**

- Bulletin de sécurité Cisco du 01-02-2023

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL>

- CVE-2023-20076

<https://www.cve.org/CVERecord?id=CVE-2023-20076>