



## BULLETIN DE SECURITE

**Titre : Vulnérabilités dans certains produits Cisco**

**Numéro de Référence : 21221807/19**

**Risque : Important**

**Impact : Important**

### Systemes affectés

- Cisco Vision Dynamic Signage Director versions antérieures à 5.0sp9
- Cisco Vision Dynamic Signage Director versions 6.0.x et 6.1.x antérieures à 6.1sp3
- Cisco FindIT Network Management versions antérieures à 2.0
- Cisco IOS Access Points (APs) versions antérieures à 8.2.170.0
- Cisco IOS Access Points (APs) versions 8.3.x antérieures à 8.3.150.0
- Cisco IOS Access Points (APs) versions 8.4.x et 8.5.x antérieures à 8.5.131.0
- Cisco IOS Access Points (APs) versions 8.6.x et 8.7.x antérieures à 8.8.100.0

### Identificateurs externes

- CVE-2019-1917 CVE-2019-1919 CVE-2019-1920 CVE-2019-1649
- CVE-2019-1919 CVE-2019-1904 CVE-2018-0473

### Bilan de la vulnérabilité

Une vulnérabilité a été corrigée dans certains produits Cisco. L'exploitation de ces failles pourrait permettre à un attaquant d'exécuter du code arbitraire à distance, de causer un déni de service à distance et de réussir un contournement de la politique de sécurité.

### Solution :

Veillez-vous référer au Bulletin de sécurité Cisco du 18 Juillet 2019.

- <https://tools.cisco.com/security/center/publicationListing.x>

### Risque :

- Exécution du code arbitraire à distance ;

- Déni de service à distance ;
- Contournement de la politique de sécurité.

**Référence :**

Bulletin de sécurité Cisco du 18 Juillet 2019.

- <https://tools.cisco.com/security/center/publicationListing.x>