



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant plusieurs produits de Cisco
<b>Numéro de Référence</b>	42660607/23
<b>Date de publication</b>	06 Juillet 2023
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- Cisco ACI Multi-Site CloudSec Encryption
- Cisco BroadWorks
- Cisco Duo Authentication Proxy
- Cisco Webex Meetings

### Identificateurs externes

- CVE-2023-20185    CVE-2023-20210    CVE-2023-20207    CVE-2023-20133  
  CVE-2023-20180

### Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'accéder à des informations confidentielles ou d'élever ses privilèges.

### Solution

Veillez se référer aux bulletins de sécurité de Cisco pour mettre à jours vos équipements.

## Risques

- Accès à des informations confidentielles
- Elévation de privilèges

## Références

Bulletins de sécurité de Cisco :

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-privesc-yw4ekrXW>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-auth-info-JgkSWBLz>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sxsscrf-2L24bBx6>