



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant des produits de Cisco
<b>Numéro de Référence</b>	53630304/25
<b>Date de publication</b>	03 Avril 2025
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- Cisco Meraki MX and Z Series AnyConnect VPN
- Cisco Enterprise Chat and Email
- Cisco Evolved Programmable Network Manager and Cisco Prime Infrastructure

### Identificateurs externes

- CVE-2025-20212 CVE-2025-20139 CVE-2025-20120 CVE-2025-20203

### Bilan de la vulnérabilité

Cisco annonce la correction de quatre vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du contenu dans une page ou de causer un déni de service.

### Solution

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

## Risques

- Injection de contenu dans une page
- Déni de service

## Références

Bulletins de sécurité de Cisco :

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vNRpDvfb>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-tC6m9GZ8>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnmpi-sxss-GSScPGY4>