



BULLETIN DE SECURITE

Titre	Vulnérabilités dans des produits Cisco
Numéro de Référence	23861903/20
Risque	Important
Impact	Important

Systemes affectés

Ces vulnérabilités affectent les produits Cisco suivants s'ils exécutent une version de Cisco SD-WAN antérieure à 19.2.2:

- Cisco vBond Orchestrator Software ;
- Cisco vEdge 100 Series Routers ;
- Cisco vEdge 1000 Series Routers ;
- Cisco vEdge 2000 Series Routers ;
- Cisco vEdge 5000 Series Routers ;
- Cisco vEdge Cloud Router Platform;
- Cisco vManage Network Management System;
- Cisco vSmart Controller Software ;

Identificateurs externes

- CVE-2020-3265 CVE-2020-3266 CVE-2020-3264 CVE-2019-16010 CVE-2019-16012

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités dans certains de ses produits. L'exploitation de ces failles peut permettre à un attaquant d'avoir les privilèges d'un utilisateur « root » et d'exécuter des commandes à distance.

Solution

Veillez-vous référer aux bulletins de sécurité Cisco du 18 Mars 2020.

Risque :

- Elévation de privilèges ;
- Exécution de commande à distance ;

Annexe

Bulletins de sécurité Cisco du 18 Mars 2020 :

- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwpresc-ySJGvE9>
- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwclicicvrQpH9v>
- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwpresc-ySJGvE9>
- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwclicicvrQpH9v>
- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanbo-QKcABnS2>
- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200318-ymanage-xss>