



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Cisco
Numéro de Référence	49441309/24
Date de Publication	13 Septembre 2024
Risque	Critique
Impact	Critique

Systemes affectés

- ConfD versions 7.5.x antérieures à 7.5.10.2
- ConfD versions 7.7.x antérieures à 7.7.16
- ConfD versions 8.0.x antérieures à 8.0.13
- Crosswork NSO versions 5.5.x antérieures à 5.5.10.1
- Crosswork NSO versions 5.6.x antérieures à 5.6.14.3
- Crosswork NSO versions 5.7.x antérieures à 5.7.16
- Crosswork NSO versions 5.8.x antérieures à 5.8.13.1
- Crosswork NSO versions 6.0.x antérieures à 6.0.13
- Crosswork NSO versions 6.1.x antérieures à 6.1.9
- Crosswork NSO versions 6.2.x antérieures à 6.2.3
- IOS XR versions 24.4.x antérieures à 24.4.1
- IOS XR versions postérieures à 24.1.x et antérieures à 24.2.2
- IOS XR versions postérieures à 7.10.x antérieures à 7.11.21
- Optical Site Manager versions antérieures à 24.3.1
- Routed Passive Optical Network Controller versions antérieures à 24.4.1

Identificateurs externes

- CVE-2024-20304 CVE-2024-20317 CVE-2024-20381 CVE-2024-20398
- CVE-2024-20406 CVE-2024-20483 CVE-2024-20489

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Cisco susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de réussir une élévation de privilèges, de contourner la politique de sécurité, d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité des données.

Solution

Veillez se référer au bulletin de sécurité Cisco du 11 septembre 2024, afin d'installer les dernières mises à jour.

Risque

- Elévation de privilèges
- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité
- Déni de service à distance
- Atteinte à la confidentialité des données

Références

Bulletin de sécurité Cisco du 11 septembre 2024:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ponctlr-ci-OHcHmsFL>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-priv-esc-CrG5vhCq>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-xehpbVNe>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-l2services-2mvHdNuC>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-auth-bypass-QnTEesp>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pak-mem-exhst-3ke9FeFy>