ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Cisco
Numéro de Référence	49022808/24
Date de Publication	29 août 2024
Risque	Important
Impact	Important

Systèmes affectés

- Small Business SPA300 Series toutes versions
- Cisco UCS version 4.2
- Cisco UCS version 4.3
- Cisco Nexus 3000 et 7000 Series Switches et Nexus 9000 Series:
    - si toutes les conditions suivantes sont remplies :
        - Ils exécutent la version 8.2(11), 9.3(9) ou 10.2(1) du logiciel Cisco NX-OS.
        - L'agent de relais DHCPv6 est activé.
        - Ils ont au moins une adresse IPv6 configurée sur le périphérique.

Identificateurs externes

- CVE-2024-20446 CVE-2024-20284 CVE-2024-20285
- CVE-2024-20286 CVE-2024-20411 CVE-2024-20413
- CVE-2024-20478 CVE-2024-20279 CVE-2024-20289

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Cisco susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, de contourner la politique de sécurité et de réussir une injection du code arbitraire.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 28 août 2024, afin d'installer les dernières mises à jour.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Déni de service
- Injection du code arbitraire
- Contournement de la politique de sécurité

Références

Bulletin de sécurité Cisco du 28 août 2024:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmdinj-Lq6jsZhH
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-psbe-ce-YvbTn5du
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bshacepe-bApeHSx7
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-priv-esc-uYQJjnuU
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cousmo-uBpBYGbq