ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits de Cisco
Numéro de Référence	46350703/24
Date de publication	07 Mars 2024
Risque	Important
Impact	Important

Systèmes affectés

- Cisco Secure Client Carriage
- Cisco Secure Client for Linux with ISE Posture Module
- Cisco AppDynamics Controller
- Cisco Small Business 100, 300, and 500 Series Wireless Access Points
- Cisco Duo Authentication for Windows

Identificateurs externes

CVE-2024-20292 CVE-2024-20301 CVE-2024-20335 CVE-2024-20336
CVE-2024-20337 CVE-2024-20338 CVE-2024-20345 CVE-2024-20346

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'élever ses privilèges de contourner les mesures de sécurité ou d'accéder à des informations confidentielles.

Solution

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

Risques

- Elévation de privilèges
- Contournement de mesures de sécurité
- Accès à des informations confidentielles

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-traversal-m7N8mZpF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-xss-3JwqSMNT
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-infodisc-rLCEqm6T
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-win-bypass-pn42KKBm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-85G83CRB
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-privesc-sYxQO6ds

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma