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



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

BULLETIN DE SECURITE

Titre	Publication de l'exploit pour une vulnérabilité affectant Cisco AnyConnect Secure Mobility Client Software et Cisco Secure Client Software
Numéro de Référence	42572306/23
Date de publication	23 Juin 2023
Risque	Important
Impact	Important

Systèmes affectés

- Cisco AnyConnect Secure Mobility Client Software pour Windows
- Cisco Secure Client Software pour Windows.

Identificateurs externes

CVE-2023-20178

Bilan de la vulnérabilité

Cisco annonce la publication de l'exploit pour une vulnérabilité affectant ses produits Cisco AnyConnect Secure Mobility Client Software et Cisco Secure Client Software. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'élever ses privilèges.

Solution

Veuillez se référer au bulletin de sécurité de Cisco pour mettre à jours vos équipements.

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: 47 21 75 37 05 فاكس: 53 20 57 77 65 05 البريد الإلكتروني contact@macert.gov.ma

Risques

• Elévation de privilèges

Références

Bulletins de sécurité de Cisco:

 $\bullet \quad \underline{https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-csc-privesc-wx4U4Kw} \\$

Tél: 05 37 57 21 47 – Fax: 05 37 57 20 53 Email: contact@macert.gov.ma