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	39761301/23
Date de Publication	13 janvier 2023
Risque	Important
Impact	Important

Systèmes affectés

- Cisco BroadWorks Application Delivery Platform Device Management versions 22.0 sans les correctifs de sécurité ADP_Rel_2022.11_1.273 et dms_2022.11_1.273
- Cisco BroadWorks Xtended Services Platform version 23.0 sans les correctifs de sécurité AP.xsp.23.0.1075.ap384245 et AP.platform.23.0.1075.ap384245
- Cisco BroadWorks Xtended Services Platform version 22.0
- Cisco Industrial Network Director (IND) versions antérieures à 1.7.0
- Cisco SIP sur les téléphones IP des séries 7800 et 8800 versions antérieures à 14.1(1)SR2
- Cisco SIP sur les téléphones IP sans-fil 8821 versions antérieures à 11.0(6)SR4
- Routeurs Cisco Small Business RV016, RV042, RV042G et RV082 (Cisco indique que ces routeurs sont en fins de vie)

Identificateurs externes

- CVE-2023-20020, CVE-2023-20037, CVE-2023-20038, CVE-2023-20018, CVE-2023-20025, CVE-2023-20026

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Cisco susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 11 janvier 2023 pour plus d'information.

Risque

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

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

Annexe

Bulletins de sécurité Cisco du 11 janvier 2023 :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ind-fZyVjJtG
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-dos-HpkeYzp

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