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	43630709/23
Date de publication	07 Septembre 2023
Risque	Important
Impact	Important

Systèmes affectés

- Cisco BroadWorks Application Delivery Platform and Xtended Services Platform
- Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers
- Cisco Identity Services Engine
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software
- Cisco HyperFlex HX Data Platform

Identificateurs externes

CVE-2023-20238 CVE-2023-20243 CVE-2023-20250 CVE-2023-20193
CVE-2023-20194 CVE-2023-20269 CVE-2023-20263

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 de causer un déni de service.

Solution

Veuillez se référer aux bulletins 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 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risques

- Elévation de privilèges
- Contournement de mesures de sécurité
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-auth-bypass-kCggMWhX
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radius-dos-W7cNn7gt
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-stack-SHYv2f5N
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-KJLp2Aw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-redirect-UxLgqdUF