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	34221301/22
Date de publication	13 Janvier 2022
Risque	Important
Impact	Important

Systèmes affectés

- Cisco Unified Contact Center Management Portal and Unified Contact Center Domain Manager
- Cisco Prime Infrastructure and Evolved Programmable Network Manager
- Cisco Tetration
- Cisco Secure Network Analytics
- Cisco Adaptive Security Device Manager
- Cisco Security Manager Cross-Site Scripting
- Cisco Enterprise Chat and Email
- Cisco IP Phones Information
- Cisco Prime Access Registrar Appliance

Pour plus d'informations sur les versions affectées veuillez consulter les bulletins de sécurité de Cisco dans la section références de ce bulletin.

Identificateurs externes

CVE-2022-20656 CVE-2022-20657 CVE-2022-20658 CVE-2022-20652
CVE-2022-20663 CVE-2022-20651 CVE-2022-20635 CVE-2022-20636
CVE-2022-20637 CVE-2022-20638 CVE-2022-20639 CVE-2022-20640
CVE-2022-20641 CVE-2022-20642 CVE-2022-20643 CVE-2022-20644
CVE-2022-20645 CVE-2022-20646 CVE-2022-20647

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 distant de contourner la politique de sécurité, d'injecter du contenu dans une page ou d'accéder à des informations confidentielles ou d'élever ses privilèges.

Solution

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

Risques

- Contournement de la politique de sécurité
- Injection de contenu dans une page
- Accès à des informations confidentielles
- Elévation de privilèges

Références

Bulletins de sécurité de Cisco :

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmp-priv-esc-JzhTFLm4
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-path-trav-zws324yn
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tetr-cmd-injc-skrwGO
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-xss-NXOxDhRQ
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-logging-jnLOY422
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-mult-xss-7hmOKQTt
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-multivulns-kbK2yVhR
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-info-disc-fRdJfOxA
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-reg-xss-zLOz8PfB

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