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	39020411/22
Date de publication	04 Novembre 2022
Risque	Important
Impact	Important

Systèmes affectés

- Cisco Identity Services Engine
- Cisco BroadWorks CommPilot
- Cisco Email Security Appliance, Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance
- Cisco Umbrella

Identificateurs externes

CVE-2022-20961 CVE-2022-20951 CVE-2022-20958 CVE-2022-20956
CVE-2022-20867 CVE-2022-20868 CVE-2022-20960 CVE-2022-20942
CVE-2022-20969 CVE-2022-20937 CVE-2022-20963 CVE-2022-20772
CVE-2022-20962

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 d'exécuter du code arbitraire, d'accéder à des informations confidentielles, d'injecter du contenu dans une page ou de contourner les mesures de sécurité.

Solution

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

Risques

- Contournement de mesures de sécurité
- Injection de contenu dans une page
- Exécution de code arbitraire
- Accès à des informations confidentielles

Références

Bulletins de sécurité de Cisco :

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-ssrf-BJeQfpp
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-access-contol-EeufSUCx
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-gdghHmbV
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-xss-LfeYQV3
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sec-atk-dos-zw5RCUYp
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stor-xss-kpRBWXY
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-path-trav-f6M7cs6r

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

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