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 critiques affectant plusieurs produits de Cisco
Numéro de Référence	41951805/23
Date de publication	18 Mai 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Cisco Small Business Series Switches
- Cisco Identity Services Engine
- Cisco Smart Software Manager
- Cisco Identity Services Engine
- Cisco DNA Center Software API
- Cisco Business Wireless Access Points

Identificateurs externes

CVE-2023-20003, CVE-2023-20024, CVE-2023-20156, CVE-2023-20157, CVE-2023-20158, CVE-2023-20159, CVE-2023-20160, CVE-2023-20161, CVE-2023-20162, CVE-2023-20189 CVE-2023-20077, CVE-2023-20087, CVE-2023-20106, CVE-2023-20171, CVE-2023-20172 CVE-2023-20110, CVE-2023-20163, CVE-2023-20164, CVE-2023-20166, CVE-2023-20167 CVE-2023-20173, CVE-2023-20174, CVE-2023-20182, CVE-2023-20183, CVE-2023-20184

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. Certaines de ces vulnérabilités sont activement exploitées et elles peuvent permettre à un attaquant distant d'exécuter du code arbitraire, de contourner des mesures de sécurité ou d'accéder à des données confidentielles.

Solution

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

Risques

- Exécution de code arbitraire
- Contournement de mesures de sécurité
- Accès à des données confidentielles

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-sql-X9MmjSYh
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-traversal-ZTUgMYhu
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-multiple-kTQkGU3
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-dwnld-Srcdnkd2
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ