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	42240806/23
Date de publication	08 Juin 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Cisco Expressway Series and Cisco TelePresence Video Communication
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances
- Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability - SIR: High
- Cisco Unified Communications Manager IM & Presence Service
- Cisco Small Business 200, 300, and 500 Series Switches
- Cisco Secure Workload

Identificateurs externes

CVE-2023-20006 CVE-2023-20105 CVE-2023-20192 CVE-2023-20108 CVE-2023-20116 CVE-2023-20136 CVE-2023-20178 CVE-2023-20188

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilité peut permettre à un attaquant d'injecter du code dans une page d'élever ses privilèges ou de causer un déni de service.

Solution

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

Risques

- Injection de code dans une page
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-priv-esc-Ls2B9t7b
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ssl-dos-uu7mV5p6
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-csc-privesc-wx4U4Kw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-dos-49GL7rzT
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-dos-4Ag3yWbD
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-sxss-OPYJZUmE
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-auth-openapi-kTndjdNX