ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Cisco
Numéro de Référence	44620311/23
Date de Publication	03 Novembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco Adaptive Security Appliance (ASA), se référer au site de l'éditeur pour vérifier les versions vulnérables (cf. section Documentation)
- Cisco Firepower Management Center (FMC), se référer au site de l'éditeur pour vérifier les versions vulnérables (cf. section Documentation)
- Cisco Firepower Threat Defense (FTD), se référer au site de l'éditeur pour vérifier les versions vulnérables (cf. section Documentation)
- Cisco Identity Services Engine (ISE) versions 3.0.x antérieures à 3.0P8
- Cisco Identity Services Engine (ISE) versions 3.1.x antérieures à 3.1P8 (annoncée courant novembre 2023, la vulnérabilité CVE-2023-20213 est corrigée dans la version 3.1P6)
- Cisco Identity Services Engine (ISE) versions 3.2.x antérieures à 3.2P3
- Cisco Identity Services Engine (ISE) versions antérieures à 2.7P10

Identificateurs externes

- CVE-2023-20048 CVE-2023-20063 CVE-2023-20083 CVE-2023-20086 CVE-2023-20095 CVE-2023-20155 CVE-2023-20170 CVE-2023-20175 CVE-2023-20195 CVE-2023-20196 CVE-2023-20213 CVE-2023-20219 CVE-2023-20220 CVE-2023-20244

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits Cisco susmentionnés. Un attaquant pourrait exploiter ces failles afin de causer un déni de service, d'exécuter du code arbitraire à distance, de réussir une élévation de privilège ou de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 01 Novembre 2023 pour plus d'information.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Exécution du code arbitraire à distance
- Elévation de privilèges
- Contournement de la politique de sécurité

Annexe

Bulletins de sécurité Cisco du 01 Novembre 2023:

- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-fmc-cmd-inj-29mp49hn
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-asa-icmpv6-t5tzqwnd
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-asa-webvpn-dos-3ghzqbas
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-fmc-cmdinj-btegufox
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-fmc-logview-dos-ayjdex55
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-ftd-fmc-code-inj-wshrgz8l
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-ftd-icmpv6-dos-4emklun
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-ftd-intrusion-dos-dft7wygc
- https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-ise-file-upload-fcelp4xs