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 dans les produits Cisco
Numéro de Référence	37741108/22
Date de Publication	11 Aout 2022
Risque	Important
Impact	Important

Systèmes affectés

- Cisco ASDM version antérieure à 7.18.1.152
- Cisco ASA antérieure à la version 9.16.3.19, à la version 9.17.1.13 ou à la version 9.18.2
- Cisco ASA avec une configuration vulnérable de « AnyConnect SSL VPN et Clientless SSL VPN »
- ASA 5506-X with FirePOWER Services
- ASA 5506H-X with FirePOWER Services
- ASA 5506W-X with FirePOWER Services
- ASA 5508-X with FirePOWER Services
- ASA 5516-X with FirePOWER Services
- Firepower 1000 Series Next-Generation Firewall
- Firepower 2100 Series Security Appliances
- Firepower 4100 Series Security Appliances
- Firepower 9300 Series Security Appliances
- Secure Firewall 3100

Identificateurs externes

- CVE-2021-1585, CVE-2022-20829, CVE-2022-20713, CVE-2022-20866, CVE-2022-20715

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Cisco susmentionnés. L'exploitation de ces failles permet à un attaquant d'exécuter du code arbitraire, de causer un déni de service, de porter atteinte aux informations confidentielles ou de réussir une élévation de privilèges.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 10 Aout 2022, afin d'installer les dernières mises à jour.

Risque

- Exécution du code arbitraire
- Déni de service
- Atteinte aux informations confidentielles

Références

Bulletin de sécurité Cisco du 10 Aout 2022:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-webvpn-LOeKsNmO
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma