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	47602305/24
Date de Publication	23 Mai 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco Firepower Management Center Software
- Cisco Adaptive Security Appliance
- Firepower Threat Defense Software
- Snort Intrusion Prevention System (IPS)

Identificateurs externes

- CVE-2024-20363, CVE-2023-20239, CVE-2024-20361, CVE-2024-20293, CVE-2024-20261, CVE-2024-20355

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, de réussir une élévation de privilège, d'injecter des requêtes SQL ou de contourner les mesures de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 22 Mai 2024 pour plus d'information.

Risque

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

Annexe

Bulletins de sécurité Cisco du 22 Mai 2024:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs

- 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-asaftd-dos-nJVAwOeq
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-ips-bypass-uE69KBMd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-archive-bypass-z4wQjwcN
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-object-bypass-fTH8tDjq
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-saml-bypass-KkNvXyKW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ogsnsg-aclbyp-3XB8q6jX