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	Produits de Cisco affectés par la vulnérabilité critique dans le serveur SSH d'Erlang/OTP
Numéro de Référence	54132304/25
Date de Publication	23 Avril 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Cisco ConfD, ConfD Basic
- Cisco Network Services Orchestrator (NSO)

Plusieurs autres produits sont sous investigation de Cisco. Veuillez se référer au bulletin de sécurité de Cisco pour rester à jour concernant la situation de ces produits.

Identificateurs externes

- CVE-2025-32433

Bilan de la vulnérabilité

Cisco annonce que la vulnérabilité critique affectant l'implémentation du serveur SSH d' Erlang concerne plusieurs de ses produits. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant non authentifié d'exécuter des commandes arbitraires

Solution

Veuillez se référer au bulletin de sécurité de Cisco afin d'installer la nouvelle mise à jour

Risque

- Exécution de commandes arbitraires à distance

Références

Bulletin de sécurité d'Erlang :

- https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

Bulletin de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy