



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans le protocole UDP
Numéro de Référence	46762803/24
Date de Publication	28 Mars 2024
Risque	Critique
Impact	Critique

Systemes affectés

- Protocole UDP (User Datagram Protocol)

Identificateurs externes

- CVE-2024-2169

Bilan de la vulnérabilité

Des chercheurs en sécurité ont révélé une vulnérabilité critique (CVE-2024-2169) affectant les implémentations du protocole UDP (User Datagram Protocol). L'exploitation réussie de cette vulnérabilité pourrait permettre à un attaquant de mener des attaques par déni de service en boucle en procédant à l'usurpation d'adresse IP, amenant deux serveurs à communiquer continuellement l'un avec l'autre en utilisant un protocole basé sur UDP. La vulnérabilité affecte les implémentations des protocoles d'application basés sur UDP, y compris le DNS, NTP, TFTP, Echo (RFC862), Chargen (RFC864), et QOTD (RFC865).

Il est conseillé aux administrateurs de systèmes utilisant des implémentations vulnérables d'UDP de mettre à jour immédiatement vers les dernières versions.

Solution

Veuillez se référer au bulletin de sécurité CERT/CC pour plus d'information.

Risque

- Déni de service

Annexe

Bulletin de sécurité CERT/CC :

- <https://www.kb.cert.org/vuls/id/417980>