



BULLETIN DE SECURITE

Titre	Vulnérabilités dans le DNS BIND
Numéro de Référence	42512206/23
Date de Publication	22 Juin 2023
Risque	Important
Impact	Important

Systemes affectés

- BIND versions 9.16.33 à 9.16.41 antérieures à 9.16.42
- BIND versions 9.18.7 à 9.18.15 antérieures à 9.18.16
- BIND versions 9.19.0 à 9.19.13 antérieures à 9.19.14
- BIND Supported Preview Edition versions 9.11.3-S1 à 9.16.41-S1 antérieures à 9.16.42-S1
- BIND Supported Preview Edition versions 9.18.11-S1 à 9.18.15-S1 antérieures à 9.18.16-S1

Identificateurs externes

- CVE-2022-38178 , CVE-2022-3924 , CVE-2023-2828 , CVE-2023-2829 , CVE-2023-2911

Bilan de la vulnérabilité

Internet Systems Consortium (ISC) a publié un correctif de sécurité qui corrige plusieurs vulnérabilités dans les versions susmentionnées de DNS BIND. L'exploitation de ces failles peut permettre à un attaquant distant de causer un déni de service.

Solution

Veillez se référer au bulletin de sécurité ISC du 21 juin 2023.

Risque

- Déni de service à distance,

Annexe

Bulletins de sécurité Internet Systems Consortium (ISC) du 21 juin 2023:

- <https://kb.isc.org/v1/docs/cve-2023-2911>
- <https://kb.isc.org/v1/docs/cve-2023-2829>
- <https://kb.isc.org/v1/docs/cve-2023-2828>