



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans le DNS BIND
<b>Numéro de Référence</b>	43952209/23
<b>Date de Publication</b>	22 Septembre 2023
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- BIND versions 9.2.0 à 9.16.43 antérieures à 9.16.44
- BIND versions 9.18.0 à 9.18.18 antérieures à 9.18.19
- BIND versions 9.19.0 à 9.19.16 antérieures à 9.19.17
- BIND édition Supported Preview versions 9.9.3-S1 à 9.16.43-S1 antérieures à 9.16.44-S1
- BIND édition Supported Preview versions 9.18.0-S1 à 9.18.18-S1 antérieures à 9.18.19-S1

### Identificateurs externes

- CVE-2023-3341, CVE-2023-4236

### 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 20 septembre 2023.

### Risque

- Déni de service à distance,

### Annexe

Bulletins de sécurité Internet Systems Consortium (ISC) du 20 septembre 2023:

- <https://kb.isc.org/v1/docs/cve-2023-4236>
- <https://kb.isc.org/v1/docs/cve-2023-3341>