

# Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Les informations](#)

[Informations connexes](#)

## Introduction

Les liens fournis dans ce document peuvent vous aider à dépanner le problème lié « Microsoft au ver SQL /Slammer/Sapphire ».

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Les informations

Le ver de Slammer a libéré en janvier 25, 2003 a eu dans le monde entier une incidence grave sur le trafic Internet. Il y a un certain nombre de technologies de sécurité de réseau Cisco intégré qui peuvent aider des organismes en réponse à ce ver et les atténuer contre de futures infestations. Ce livre blanc et l'accompagnement de la présentation Par script aideront en communiquant aux clients les moyens de combattre des vers Internet utilisant la Sécurité de réseau intégré.

- Note de sécurité Cisco : Recommandations de réduction de ver de Microsoft

SQL <http://www.cisco.com/en/US/products/csa/cisco-sa-20030125-worm.html>

- Avis de sécurité Cisco : Vulnérabilités de Microsoft SQL Server 2000 dans des Produits Cisco - MS02-061 <http://www.cisco.com/en/US/products/csa/cisco-sa-20030126-ms02-061.html>

## **Informations connexes**

- [Avis de sécurité Cisco, réponses, et notices](#)
- [Support et documentation techniques - Cisco Systems](#)