

# Microsoft SQL /Slammer/Sapphire索引

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[資訊](#)

[相關資訊](#)

## 簡介

本文檔中提供的連結可幫助您解決與「Microsoft SQL /Slammer/Sapphire」蠕蟲相關的問題。

## [必要條件](#)

### [需求](#)

本文件沒有特定需求。

### [採用元件](#)

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### [慣例](#)

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## [資訊](#)

2003年1月25日發佈的Slammer蠕蟲對全世界的網際網路流量造成了嚴重影響。有許多思科整合網路安全技術可以幫助組織響應此蠕蟲病毒並減輕未來感染的風險。本白皮書和隨附的指令碼演示將幫助向客戶傳達使用整合網路安全來打擊Internet蠕蟲的方法。

- 思科安全宣告：Microsoft SQL蠕蟲緩解建議<http://www.cisco.com/en/US/products/csa/cisco-sa-20030125-worm.html>
- 思科資安顧問諮詢：思科產品中的Microsoft SQL Server 2000漏洞 — MS02-

## **相關資訊**

- [思科資安諮詢、回應和通知](#)
- [技術支援與文件 - Cisco Systems](#)