# Comment protéger votre réseau contre le virus Nimda

## Contenu



## Introduction

Ce document décrit les moyens de minimiser l'impact du ver Nimda sur votre réseau. Ce document aborde deux sujets :

- Le réseau est infecté, que peut-on faire ? Comment pouvez-vous minimiser les dégâts et les retombées ?
- Le réseau n'est pas encore infecté ou n'est que partiellement infecté. Que peut-on faire pour minimiser la propagation de ce ver ?

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

# Informations générales

Pour obtenir des informations générales sur le ver Nimda, reportez-vous aux liens suivants :

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

# Plates-formes prises en charge

La solution NBAR (Network-Based Application Recognition) décrite dans ce document nécessite la fonctionnalité de marquage par classe du logiciel Cisco IOS®. Et plus particulièrement, la capacité de faire correspondre sur n'importe quelle partie d'une adresse URL HTTP, la fonction de classification de port secondaire HTTP à l'intérieur d'une NBAR. Les plates-formes compatibles et les spécifications minimum requises pour le logiciel Cisco IOS sont récapitulées ci-dessous :

| Plateforme | Version logicielle Cisco IOS minimale |
|---|---|
| 7200 | 12.1(5)T |
| 7100 | 12.1(5)T |
| 3660 | 12.1(5)T |
| 3640 | 12.1(5)T |
| 3620 | 12.1(5)T |
| 2600 | 12.1(5)T |
| 1700 | 12.2(5)T |

**Remarque :** vous devez activer Cisco Express Forwarding (CEF) afin d'utiliser NBAR (Network-Based Application Recognition).

NBAR est également pris en charge sur certaines plates-formes logicielles Cisco IOS à partir de la version 12.1E. Voir « Protocoles pris en charge » dans la documentation de reconnaissance des applications réseau.

Le marquage basée sur les classes et les NBAR distribués (DNBAR) sont également disponibles sur les plates-formes suivantes :

| Plateforme | Version logicielle Cisco IOS minimale |
|---|---|
| 7500 | 12.1(6)E |
| FlexWAN | 12.1(6)E |

Si vous déployez NBAR, soyez conscient de l'ID de bogue Cisco CSCdv06207 (clients enregistrés uniquement). La solution de contournement décrite dans CSCdv06207 peut être nécessaire si vous rencontrez ce défaut.

La solution ACL (Access Control List) est prise en charge dans toutes les versions actuelles du logiciel Cisco IOS.

Pour les solutions pour lesquelles vous devez utiliser l'interface de ligne de commande (CLI) QoS (Modular Quality of Service) (par exemple pour limiter le trafic ARP ou pour implémenter la limitation de débit avec le régulateur au lieu du CAR), vous avez besoin de l'interface de ligne de commande Qualité de service modulaire disponible dans le logiciel Cisco IOS versions 12.0XE, 12.1E, 11T, et toutes les versions du 12.2.

Pour utiliser le CAR (Committed Access Rate), vous avez besoin du logiciel Cisco IOS version 11.1CC et de toutes les versions du logiciel 12.0 et des versions ultérieures.

## Comment minimiser les dommages et limiter les retombées

Cette section décrit les vecteurs d'infection qui peuvent propager le virus Nimda et fournit des conseils pour réduire la propagation du virus :

- Le ver peut se propager par le biais de pièces jointes par e-mail du type MIME audio/x-wav.**Conseils :**Ajoutez des règles sur votre serveur SMTP (Simple Mail Transfer Protocol) pour bloquer tout e-mail comportant ces pièces jointes :readme.exeAdmin.dll
- Le ver peut se propager lorsque vous naviguez sur un serveur web infecté avec l'exécution Javascript activée et en utilisant une version d'Internet Explorer (IE) qui est vulnérable aux exploits discutés dans MS01-020 (par exemple, IE 5.0 ou IE 5.01 sans SP2).**Conseils :**Utilisez Netscape comme navigateur, ou désactivez Javascript sur IE, ou obtenez un correctif IE à SP II.Utilisez la fonction de reconnaissance des applications réseau (NBAR) de Cisco pour filtrer les fichiers readme.eml à partir du téléchargement. Voici un exemple de configuration de NBAR :
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Une fois que vous avez mis en correspondance le trafic, vous pouvez choisir de supprimer ou de router le trafic basé sur des stratégies pour surveiller les hôtes infectés. Des exemples de la mise en oeuvre complète se trouvent dans Utilisation de listes de contrôle d'accès et de reconnaissance d'applications basées sur le réseau pour bloquer le ver « Code Red ».
- Le ver peut se propager d'une machine à l'autre sous la forme d'attaques IIS (il tente principalement d'exploiter les vulnérabilités créées par les effets de Code Red II, mais aussi les vulnérabilités précédemment corrigées par MS00-078 ).**Conseils :**Utilisez les schémas Code Red décrits à la section :Réponse à un cas d'erreur mallocfail ou d'utilisation élevée du processeur résultant du ver « Code Red »Utilisation de listes de contrôle d'accès et de reconnaissance d'applications basées sur le réseau pour bloquer le ver « Code Red »
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*.ida*"
  Router(config-cmap)#match protocol http url "*cmd.exe*"
  Router(config-cmap)#match protocol http url "*root.exe*"
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Une fois que vous avez mis en correspondance le trafic, vous pouvez choisir de supprimer ou de router le trafic basé sur des stratégies pour surveiller les hôtes infectés. Des exemples de la mise en oeuvre complète se trouvent dans Utilisation de listes de contrôle d'accès et de reconnaissance d'applications basées sur le réseau pour bloquer le ver « Code Red ».Paquets SYN (Rate-limit TCP synchronize/start). Cela ne protège pas un hôte, mais permet à votre réseau de fonctionner de manière dégradée et de rester toujours actif. En limitant les SYN, vous jetez des paquets qui dépassent un certain débit, de sorte que certaines connexions TCP passent, mais pas toutes. Pour des exemples de configuration, reportez-vous à la section « Rate Limitation for TCP SYN Packets » de Using CAR When DOS

Attacks.Envisagez de limiter le trafic ARP (Address Resolution Protocol) si la quantité d'analyses ARP cause des problèmes sur le réseau. Pour limiter le trafic ARP, configurez les éléments suivants :

```
class-map match-any arp
   match protocol arp
!
!
policy-map ratelimitarp
   class arp
      police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```

Cette stratégie doit ensuite être appliquée à l'interface LAN appropriée en tant que stratégie de sortie. Modifiez les figures comme il convient pour tenir compte du nombre d'ARP par seconde que vous souhaitez autoriser sur le réseau.

- Le ver peut se propager en mettant en surbrillance un .eml ou .nws dans l'Explorateur avec Active Desktop activé (W2K/ME/W98 par défaut). Cela entraîne l'exécution du fichier THUMBVW.DLL et la tentative de téléchargement du fichier README.EML référencé dans ce fichier (selon votre version IE et vos paramètres de zone).**Conseil :** Comme recommandé ci-dessus, utilisez NBAR pour filtrer readme.eml à partir du téléchargement.
- Le ver peut se propager à travers les lecteurs mappés. Toute machine infectée qui possède des lecteurs réseau mappés infectera probablement tous les fichiers du lecteur mappé et de ses sous-répertoires**Conseils :**Bloquez le protocole TFTP (Trivial File Transfer Protocol) (port 69) afin que les machines infectées ne puissent pas utiliser TFTP pour transférer des fichiers vers des hôtes non infectés. Assurez-vous que l'accès TFTP pour les routeurs est toujours disponible (car vous aurez peut-être besoin du chemin pour mettre à niveau le code). Si le routeur exécute le logiciel Cisco IOS version 12.0 ou ultérieure, vous avez toujours la possibilité d'utiliser le protocole FTP (File Transfer Protocol) pour transférer des images vers des routeurs exécutant le logiciel Cisco IOS.Bloquer NetBIOS. NetBIOS ne doit pas quitter un réseau local (LAN). Les fournisseurs de services doivent filtrer NetBIOS en bloquant les ports 137, 138, 139 et 445.
- Le ver utilise son propre moteur SMTP pour envoyer des e-mails afin d'infecter d'autres systèmes.**Conseil :** bloquez le port 25 (SMTP) sur les parties internes de votre réseau. Les utilisateurs qui récupèrent leur courrier électronique à l'aide du protocole POP (Post Office Protocol) 3 (port 110) ou IMAP (Internet Mail Access Protocol) (port 143) n'ont pas besoin d'accéder au port 25. Autorisez uniquement l'ouverture du port 25 face au serveur SMTP du réseau. Cela peut ne pas être possible pour les utilisateurs utilisant Eudora, Netscape et Outlook Express, entre autres, car ils ont leur propre moteur SMTP et généreront des connexions sortantes à l'aide du port 25. Il pourrait être nécessaire d'enquêter sur les utilisations possibles de serveurs proxy ou d'un autre mécanisme.
- Nettoyer les serveurs Cisco CallManager/Applications**Conseil :** les utilisateurs disposant de serveurs d'applications Call Manager et Call Manager sur leurs réseaux doivent effectuer les opérations suivantes pour arrêter la propagation du virus. Ils ne doivent pas accéder à la machine infectée à partir du Call Manager et ne doivent pas partager de lecteurs sur le serveur Call Manager. Suivez les instructions fournies dans Nettoyer le virus Nimda à partir de Cisco CallManager 3.x et des serveurs d'applications CallManager pour nettoyer le virus Nimda.
- Filtrer le virus Nimda sur CSS 11000**Conseil :** Les utilisateurs de CSS 11000 doivent suivre les instructions fournies dans Filtrage du virus Nimda sur CSS 11000 pour nettoyer le virus NIMDA.

- Réponse de Cisco Secure Intrusion Detection System (CS IDS) au virus Nimda**Conseil :** Le système CS IDS dispose de deux composants différents. L'un est le système de détection d'hôte (HIDS) qui possède un capteur d'hôte et le système de détection d'intrusion réseau (NIDS) qui possède un capteur de réseau, qui répondent tous deux différemment au virus Nimda. Pour une explication plus détaillée et la marche à suivre recommandée, référez-vous à Comment Cisco Secure IDS répond au virus Nimda.

## Informations connexes

- Utilisation de listes de contrôle d'accès et de reconnaissance d'applications basées sur le réseau pour bloquer le ver « Code Red »
- Réponse à un cas d'erreur mallocfail ou d'utilisation élevée du processeur résultant du ver « Code Red »
- Utilisation de CAR lors d'attaques par déni de service (DoS)
- Notifications et avis de sécurité Cisco
- Support et documentation techniques - Cisco Systems