# Schutz des Netzwerks vor dem Nimda-Virus

## Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Hintergrundinformationen](#)
[Unterstützte Plattformen](#)
[Minimieren des Schadens und Begrenzen der Blende](#)
[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt Möglichkeiten, die Auswirkungen des Nimda-Wurms auf Ihr Netzwerk zu minimieren. In diesem Dokument werden zwei Themen behandelt:

- Das Netzwerk ist infiziert, was kann getan werden? Wie können Sie Schäden und Auswirkungen minimieren?
- Das Netzwerk ist noch nicht infiziert oder nur teilweise infiziert. Was kann getan werden, um die Verbreitung dieses Wurms zu minimieren?

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

# Hintergrundinformationen

Hintergrundinformationen zum Nimda-Wurm finden Sie unter den folgenden Links:

- 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

# Unterstützte Plattformen

Die in diesem Dokument beschriebene Network-Based Application Recognition (NBAR)-Lösung erfordert die klassenbasierte Markierungsfunktion in der Cisco IOS®-Software. Insbesondere die Möglichkeit, einen beliebigen Teil einer HTTP-URL abzugleichen, verwendet die HTTP-Subport-Klassifizierungsfunktion in NBAR. Die unterstützten Plattformen und die Mindestanforderungen für die Cisco IOS-Software werden nachfolgend zusammengefasst:

| Plattform | Mindestversion der Cisco IOS Software |
|---|---|
| 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 |

**Hinweis:** Sie müssen Cisco Express Forwarding (CEF) aktivieren, um Network-Based Application Recognition (NBAR) verwenden zu können.

NBAR wird ab Version 12.1E auch auf einigen Cisco IOS-Softwareplattformen unterstützt. Siehe "Unterstützte Protokolle" in der Dokumentation zur netzwerkbasierten Anwendungserkennung.

Klassenbasierte Kennzeichnung und Distributed NBAR (DNBAR) sind auch auf den folgenden Plattformen verfügbar:

| Plattform | Mindestversion der Cisco IOS Software |
|---|---|
| 7500 | 12,1(6)E |
| FlexWAN | 12,1(6)E |

Wenn Sie NBAR bereitstellen, informieren Sie sich über die Cisco Bug-ID CSCdv06207 (nur registrierte Kunden). Bei Auftreten dieses Fehlers ist möglicherweise die in CSCdv06207 beschriebene Problemumgehung erforderlich.

Die Zugriffskontrolllisten-Lösung (ACL) wird in allen aktuellen Versionen der Cisco IOS-Software unterstützt.

Für Lösungen, bei denen die modulare Quality of Service (QoS)-Befehlszeilenschnittstelle (CLI)

(z. B. für den Durchsatzbegrenzenden ARP-Datenverkehr oder für die Implementierung einer Durchsatzbegrenzung anstelle von CAR) verwendet werden muss, benötigen Sie die modulare Quality of Service Command Line Interface, die in den Cisco IOS-Softwareversionen 12.0XE, 12.1E, 1.1T und 12.1T verfügbar ist. alle Versionen von 12.2.

Für die Verwendung der Committed Access Rate (CAR) benötigen Sie die Cisco IOS Software Release 11.1CC und alle Versionen der Software 12.0 und höher.

## Minimieren des Schadens und Begrenzen der Blende

In diesem Abschnitt werden die Infektionsvektoren beschrieben, die das Nimda-Virus verbreiten können, und es werden Tipps gegeben, wie die Ausbreitung des Virus verringert werden kann:

- Der Wurm kann sich über E-Mail-Anhänge des MIME Audio/x-wav-Typs verbreiten.**Tipps:**Fügen Sie Regeln auf dem SMTP-Server (Simple Mail Transfer Protocol) hinzu, um E-Mails mit folgenden Anhängen zu blockieren:readme.exeAdmin.dll
- Der Wurm kann sich verbreiten, wenn Sie einen infizierten Webserver mit aktivierter JavaScript-Ausführung durchsuchen und eine Version von Internet Explorer (IE) verwenden, die anfällig für die in MS01-020 diskutierten Exploits ist (z. B. IE 5.0 oder IE 5.01 ohne SP2).**Tipps:**Verwenden Sie Netscape als Browser, oder deaktivieren Sie Javascript auf IE, oder lassen Sie IE gepatcht auf SP II.Verwenden Sie die netzwerkbasierte Anwendungserkennung von Cisco (NBAR), um Dateien readme.eml vom Herunterladen zu filtern. Das folgende Beispiel zeigt die Konfiguration von NBAR:
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Nach der Zuordnung des Datenverkehrs können Sie festlegen, ob der Datenverkehr verworfen oder richtlinienbasiert weitergeleitet werden soll, um infizierte Hosts zu überwachen. Beispiele für die vollständige Implementierung finden Sie unter Verwenden von netzwerkbasierten Anwendungserkennungs- und Zugriffskontrolllisten zum Blockieren des "Code Red"-Wurms.
- Der Wurm kann sich in Form von IIS-Angriffen von einem Computer zum anderen ausbreiten (er versucht in erster Linie, Schwachstellen auszunutzen, die durch die Auswirkungen von Code Red II entstanden sind, aber auch Schwachstellen, die zuvor durch MS00-078 gepatcht wurden).**Tipps:**Verwenden Sie die unter beschriebenen Code Red-Schemas:Umgang mit Mallocfail und hoher CPU-Auslastung durch den Wurm "Code Red"Verwenden von netzwerkbasierten Anwendungserkennungs- und Zugriffskontrolllisten zum Blockieren des Wurms "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*"
  ```
  Nach der Zuordnung des Datenverkehrs können Sie festlegen, ob der Datenverkehr verworfen oder richtlinienbasiert weitergeleitet werden soll, um infizierte Hosts zu überwachen. Beispiele für die vollständige Implementierung finden Sie unter Verwenden von netzwerkbasierten Anwendungserkennungs- und Zugriffskontrolllisten zum Blockieren des "Code Red"-Wurms.Übertragungsratenlimit: TCP-SYN-Pakete (Synchronize/Start) Dies schützt einen Host nicht, ermöglicht jedoch die Ausführung des Netzwerks auf eine heruntergestufte Art und Weise, die auch weiterhin besteht. Durch die Ratenbegrenzung von SYNs werden Pakete verworfen, die eine bestimmte Rate überschreiten, sodass einige TCP-

Verbindungen durchlaufen werden, aber nicht alle. Konfigurationsbeispiele finden Sie im Abschnitt "Ratenbegrenzung für TCP-SYN-Pakete" unter Verwenden von CAR bei DOS-Angriffen.Berücksichtigen Sie den ARP-Datenverkehr (Address Resolution Protocol), wenn die Anzahl der ARP-Scans Probleme im Netzwerk verursacht. Um den ARP-Datenverkehr zu begrenzen, konfigurieren Sie Folgendes:

```
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
```

Diese Richtlinie muss dann als Ausgaberichtlinie auf die entsprechende LAN-Schnittstelle angewendet werden. Ändern Sie die Zahlen entsprechend, um die Anzahl der ARPs pro Sekunde zu berücksichtigen, die im Netzwerk zugelassen werden sollen.

- Der Wurm kann sich verbreiten, indem er entweder EML oder .nws im Explorer mit aktiviertem Active Desktop markiert (W2K/ME/W98 standardmäßig). Dies bewirkt, dass die Datei THUMBVW.DLL ausgeführt wird und versucht, die darin erwähnte README.EML-Datei herunterzuladen (abhängig von der IE-Version und den Zoneneinstellungen).**Tipp:** Verwenden Sie wie oben empfohlen NBAR, um die Datei readme.eml aus dem Herunterladen zu filtern.
- Der Wurm kann sich über zugeordnete Laufwerke ausbreiten. Jeder infizierte Computer, der Netzwerklaufwerke zugeordnet hat, infiziert wahrscheinlich alle Dateien auf dem zugeordneten Laufwerk und seinen Unterverzeichnissen.**Tipps:**Trivial File Transfer Protocol (TFTP) (Port 69) wird blockiert, sodass infizierte Computer TFTP nicht verwenden können, um Dateien auf nicht infizierte Hosts zu übertragen. Stellen Sie sicher, dass der TFTP-Zugang für Router weiterhin verfügbar ist (da Sie den Pfad für die Codeaktualisierung benötigen). Wenn auf dem Router die Cisco IOS-Software (Version 12.0 oder höher) ausgeführt wird, können Sie jederzeit das File Transfer Protocol (FTP) verwenden, um Images auf Router mit Cisco IOS-Software zu übertragen.Blockieren Sie NetBIOS. NetBIOS sollte kein Local Area Network (LAN) verlassen müssen. Service Provider sollten NetBIOS-Out filtern, indem sie die Ports 137, 138, 139 und 445 blockieren.
- Der Wurm verwendet seine eigene SMTP-Engine, um E-Mails an andere Systeme zu senden.**Tipp:** Blockieren Sie Port 25 (SMTP) in den internen Bereichen Ihres Netzwerks. Benutzer, die ihre E-Mails mit Post Office Protocol (POP) 3 (Port 110) oder Internet Mail Access Protocol (IMAP) (Port 143) abrufen, benötigen keinen Zugriff auf Port 25. Lassen Sie Port 25 nur für den SMTP-Server für das Netzwerk offen. Dies ist unter anderem für Benutzer von Eudora, Netscape und Outlook Express nicht machbar, da sie über eine eigene SMTP-Engine verfügen und ausgehende Verbindungen über Port 25 generieren. Möglicherweise müssen einige Untersuchungen auf die mögliche Verwendung von Proxyservern oder anderen Mechanismen angewendet werden.
- Clean von Cisco CallManager/Anwendungsservern**Tipp:** Benutzer mit Call Manager- und Call Manager-Anwendungsservern in ihren Netzwerken müssen folgende Schritte ausführen, um die Verbreitung des Virus zu stoppen. Sie dürfen nicht vom Call Manager auf den infizierten Computer zugreifen und auch keine Laufwerke auf dem Call Manager-Server gemeinsam nutzen. Befolgen Sie die Anweisungen unter Reinigen des Nimda-Virus von Cisco CallManager 3.x- und CallManager-Anwendungsservern zum Reinigen des Nimda-Virus.
- Filtern des Nimda-Virus auf dem CSS 11000**Tipp:** Benutzer mit CSS 11000 müssen die Anweisungen unter Filtern des Nimda-Virus auf CSS 11000 befolgen, um das NIMDA-Virus

zu reinigen.
- Cisco Secure Intrusion Detection System (CS IDS) reagiert auf das Nimda-Virus**Tipp:** Das CS IDS verfügt über zwei verschiedene Komponenten. Eine davon ist das Host-basierte IDS (HIDS) mit einem Host-Sensor und das Network-Based IDS (NIDS) mit einem Netzwerksensor, die beide unterschiedlich auf den Nimda-Virus reagieren. Eine ausführlichere Erklärung und die empfohlene Vorgehensweise finden Sie unter Wie Cisco Secure IDS auf das Nimda-Virus reagiert.

## Zugehörige Informationen

- Verwenden von netzwerkbasierten Anwendungserkennungs- und Zugriffskontrolllisten zum Blockieren des Wurms "Code Red"
- Umgang mit Mallocfail und hoher CPU-Auslastung durch den Wurm "Code Red"
- Verwendung von CAR bei DOS-Angriffen
- Cisco Sicherheitsratgeber und -hinweise
- Technischer Support und Dokumentation für Cisco Systeme