Uw netwerk beschermen tegen het NIMA-virus

Inhoud

Inleiding

In dit document worden manieren beschreven om de impact van de Nimda-worm op uw netwerk te minimaliseren. Dit document richt zich op twee onderwerpen:

- Het netwerk is geïnfecteerd, wat kan er gedaan worden? Hoe kan je de schade en de neerslag tot een minimum beperken?
- Het netwerk is nog niet of slechts gedeeltelijk geïnfecteerd. Wat kan er worden gedaan om de verspreiding van deze worm tot een minimum te beperken?

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Raadpleeg voor achtergrondinformatie over de Nimda-worm deze 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

Ondersteunde platforms

De Network-Based Application Recognition (NBAR) oplossing, die in dit document wordt beschreven, vereist de op klasse gebaseerde markering binnen de software van Cisco IOS®. In het bijzonder, de mogelijkheid om op elk deel van een HTTP URL aan te passen gebruikt de HTTP sub-port classificatie optie binnen NBAR. De ondersteunde platforms en de minimale Cisco IOS-softwarevereisten worden hieronder samengevat:

platform	Minimale Cisco IOS-softwarerelease
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

Opmerking: U moet Cisco Express Forwarding (CEF) inschakelen om Network-Based Application Recognition (NBAR) te gebruiken.

NBAR wordt ook ondersteund op sommige Cisco IOS-softwareplatforms die beginnen met release 12.1E. Zie "Ondersteunde protocollen" in de netwerkgebaseerde Application Recognition-documentatie.

Op klasse gebaseerde markering en Distributed NBAR (DNBAR) zijn ook beschikbaar op de volgende platforms:

platform	Minimale Cisco IOS-softwarerelease
7500	12.1(6)E
FlexWAN	12.1(6)E

Als u NBAR implementeert, moet u zich bewust zijn van Cisco bug-ID CSCdv06207 (alleen geregistreerde klanten). Als u dit defect tegenkomt, is de in CSCdv06207 beschreven tijdelijke oplossing mogelijk nodig.

De oplossing van toegangscontrolelijst (ACL) wordt ondersteund in alle huidige releases van Cisco IOS-software.

Voor oplossingen waar u de Opdrachtinterface met modulaire Quality of Service (QoS) (CLI) moet gebruiken (zoals voor snelheidsbeperkende ARP-verkeer of voor het implementeren van

snelheidsbeperkingen met politieman in plaats van CAR), hebt u de modulaire Quality of Service Opdracht-Line Interface nodig die beschikbaar is in Cisco IOS-softwarereleases 12.0XE, 12.1E, en alle releases van 12.2.

Voor gebruik van Committed Access Rate (CAR) hebt u Cisco IOS-softwarerelease 11.1CC en alle releases van 12.0 en latere software nodig.

De schade tot een minimum beperken en de uitval beperken

In dit gedeelte worden de infectievectoren beschreven die het Nimda-virus kunnen verspreiden en worden tips gegeven om de verspreiding van het virus te verminderen:

- De worm kan zich via e-mailbijlagen van het MIME audio/x-wav type verspreiden.**Tips:**Voeg regels toe op uw Eenvoudige Server van het Protocol van de Post (mtd) om elke e-mail te blokkeren die deze bijlagen heeft:readme.exeAdmin.dll
- De worm kan zich verspreiden wanneer u door een geïnfecteerde webserver bladert met de uitvoering van Javascript en gebruik maakt van een versie van Internet Explorer (IE) die kwetsbaar is voor de explosies die in MS01-020 zijn besproken (bijvoorbeeld IE 5.0 of IE 5.01 zonder SP2).**Tips:**Gebruik Netscape als uw browser, of blokkeer Javascript op IE, of krijg IE gelapt op SP II.Gebruik Cisco Network-Based Application Recognition (NBAR) om readme.eml-bestanden te filteren vanaf het moment dat ze worden gedownload. Hier is een voorbeeld om NBAR te configureren:
  ```
  Router(config)#class-map match-any http-hacks
  Router(config-cmap)#match protocol http url "*readme.eml*"
  ```
  Nadat u het verkeer hebt aangepast, kunt u kiezen om te ontdoen of Op beleid gebaseerde Route van het verkeer om geïnfecteerde hosts te controleren. Voorbeelden van de volledige implementatie worden gevonden in het gebruik van netwerkgebaseerde Application Recognition en toegangscontrolelijsten voor het blokkeren van het "Code Red"-woord.
- De worm kan zich van machine tot machine verspreiden in de vorm van IS-aanvallen (het probeert voornamelijk kwetsbaarheden te exploiteren die zijn ontstaan door de effecten van Code Red II, maar ook kwetsbaarheden die eerder door MS00-078 zijn gepatenteerd).**Tips:**Gebruik de in:Gebruik van mallocaten en hoge CPU's als gevolg van het "coderode" wormNetwerkgebaseerde Application Recognition- en toegangscontrolelijsten voor het blokkeren van het "Code Red"-werk
  ```
  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*"
  ```
  Nadat u het verkeer hebt aangepast, kunt u kiezen om te ontdoen of Op beleid gebaseerde Route van het verkeer om geïnfecteerde hosts te controleren. Voorbeelden van de volledige implementatie worden gevonden in het gebruik van netwerkgebaseerde Application Recognition en toegangscontrolelijsten voor het blokkeren van het "Code Red"-woord.Rate-Limiet TCP-synchroniseer/start (SYN)-pakketten. Dit beschermt een host niet, maar het stelt uw netwerk in staat om op een aangetaste manier te draaien en toch op te blijven. Door snelheidsbeperkende SYNs, gooi u pakketten weg die een bepaald tempo overschrijden, zodat sommige TCP verbindingen door zullen komen, maar niet allemaal. Raadpleeg voor configuratievoorbeelden het gedeelte "Rate Limiting for TCP SYN Packets" van het gebruiken van CAR tijdens DOS aanvallen.Overweeg verkeer van het Protocol van de Resolutie van het Adres (ARP) van het tarief-Beperkend als de hoeveelheid ARP scans problemen in het

netwerk veroorzaakt. Configureer het volgende om de grenswaarde voor ARP-verkeer te bepalen:

```
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
```

Dit beleid moet dan worden toegepast op de relevante LAN-interface als een uitvoerbeleid. Wijzig de getallen zo nodig om rekening te houden met het aantal ARP's per seconde dat u op het netwerk wilt toestaan.

- De worm kan zich verspreiden door een .eml of .nws in Verkenner te markeren met Actieve Desktop ingeschakeld (W2K/ME/W98 standaard). Dit veroorzaakt dat THUMBVW.DLL het bestand wil uitvoeren en probeert het genoemde README.EML te downloaden (afhankelijk van uw IE versie en zone instellingen).**Tip:** Gebruik NBAR om readme.eml te filteren vanaf het moment dat u het uploadt.
- De worm kan zich verspreiden door de kaart. Elke besmette machine die netwerkschijven heeft ingeschakeld, infecteert waarschijnlijk alle bestanden op het gekoppelde station en de bijbehorende subdirectories**Tips:**Blok Trial File Transfer Protocol (TFTP) (poort 69) zodat besmette machines geen TFTP kunnen gebruiken om bestanden over te brengen naar niet-geïnfecteerde hosts. Zorg ervoor dat TFTP-toegang voor routers nog beschikbaar is (aangezien u het pad naar upgradecode wellicht nodig hebt). Als de router Cisco IOS-softwarerelease 12.0 of hoger draait, hebt u altijd de optie om File Transfer Protocol (FTP) te gebruiken om afbeeldingen over te brengen naar routers die Cisco IOS-software uitvoeren.Blokkeer NetReset. NetVOS hoeft geen lokaal netwerk (LAN) te verlaten. Serviceproviders moeten Netopgemerkt blijven door de poorten 137, 138, 139 en 445 te blokkeren.
- De worm maakt gebruik van zijn eigen MTP-motor om e-mails naar buiten te sturen om andere systemen te infecteren.**Tip:** Blokpoort 25 (MTP) op de binnendelen van uw netwerk. Gebruikers die hun e-mail ophalen met Post Office Protocol (POP) 3 (poort 110) of Internet Mail Access Protocol (IMAP) (poort 143) hebben geen toegang tot poort 25 nodig. Alleen toestaan dat haven 25 wordt geopend tegenover de MTP-server voor het netwerk. Dit kan niet mogelijk zijn voor gebruikers die onder andere Eudora, Netscape en Outlook Express gebruiken, aangezien zij hun eigen MTP-motor hebben en uitgaande verbindingen zullen genereren met behulp van haven 25. Een bepaald onderzoek zou kunnen worden toegepast op het mogelijke gebruik van proxy-servers of een ander mechanisme.
- Cisco CallManager/toepassingsservers reinigen**Tip:** Gebruikers met Call Managers en Call Manager toepassingsservers in hun netwerken moeten het volgende doen om de verspreiding van het virus te stoppen. Ze moeten niet naar een geïnfecteerde machine bladeren vanuit Call Manager en ze moeten ook geen schijven delen op de Call Manager server. Volg de instructies die zijn meegeleverd in het schoonmaken van het NIMA-virus uit Cisco CallManager 3.x en CallManager-toepassingsservers voor het reinigen van het NIMA-virus.
- Het Nimda-virus op de CSS 11000 filteren**Tip:** Gebruikers met CSS 11000 moeten de instructies opvolgen die worden verstrekt in Filtering van het NIMDA-virus op CSS 11000 voor het reinigen van het NIMDA-virus.
- Cisco Secure Inbraakdetectiesysteem (UCS) - reactie op het NIMA-virus**Tip:** de UCS IDS heeft twee verschillende onderdelen beschikbaar. Een daarvan is de Host-Based IDS (HIDS),

die een hostsensor en de Network-Based IDS (NIDS) heeft, die een netwerksensor heeft, die beide op een andere manier reageren op het Nimda-virus. Raadpleeg voor een gedetailleerdere uitleg en het aanbevolen verloop van de actie hoe Cisco Secure IDS reageert op het NIMA-virus.

Gerelateerde informatie

- Netwerkgebaseerde Application Recognition- en toegangscontrolelijsten voor het blokkeren van het "Code Red"-werk
- Gebruik van mallocaten en hoge CPU's als gevolg van het "coderode" worm
- CAR gebruiken tijdens DOS-aanvallen
- Cisco Security Advisories en kennisgevingen
- Technische ondersteuning en documentatie – Cisco Systems