Hoe Cisco Secure IDS reageert op het NIMA-virus

Inhoud

Inleiding

Dit document legt uit hoe Cisco Secure Inbraakdetectiesysteem (IDS) web server-compromis identificeert en voorkomt dat aanvallen door de NIMD-worm (ook bekend als het Concept-virus) worden voorkomen. De complexe technische werking van de worm valt buiten het toepassingsgebied van dit bericht en is elders goed gedocumenteerd. Een van de beste technische beschrijvingen van de Nimda worm is te vinden in CERT® Advisory CA-2001-26 Nimda Worm .

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.

Conventies

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

Achtergrondinformatie

De Nimda-worm is een hybride worm en een virus dat zich agressief verspreidt op het internet. Om Nimda en de vermogens van Cisco IDS te begrijpen om zijn verspreiding te verminderen, is het belangrijk om deze twee termen te definiëren:

- **Worm** verwijst naar kwaadaardige code die automatisch verspreid wordt, zonder menselijke interventie.
- **Virus** verwijst naar kwaadaardige code die zich door een bepaald soort menselijke interventie verspreidt, zoals wanneer u een e-mail opent, een geïnfecteerde website bladert of handmatig een besmet bestand uitvoert.

De Nimda-worm is een hybride die kenmerken van zowel een worm als een virus vertoont. Nimda infecteert op meerdere manieren, waarvan de meeste menselijke interventie vereisen. Cisco IDS Host Sensor blokkeert worm-achtige infectiemethoden die zich door kwetsbaarheden in de Internet Information Server (IS) van Microsoft verspreiden. Cisco IDS blokkeert de virusachtige, handmatige infectiemethoden niet, zoals wanneer u een e-mailbijlage opent, een geïnfecteerde website bladert of handmatig een besmet bestand uitvoert.

Cisco IDS-hostsensor biedt bescherming tegen NIMA

Cisco IDS Host Sensor voorkomt aanvallen van mappen, waartoe ook de aanslagen behoren die door de NIMA-worm worden gebruikt. Wanneer de worm probeert om een Cisco IDS-beschermde webserver in gevaar te brengen, faalt de aanval en wordt de server niet gecompromitteerd.

Deze Cisco IDS Host Sensor-regels voorkomen het succes van de Nimda-worm:

- IOS-adresomzetting (vier regels)
- IOS-adresomzetting en uitvoering van codes (vier regels)
- IS Dubbele Hex Encoding Directory Traversal (vier regels)

Cisco IDS Host Sensor verdedigt ook tegen onbevoegde veranderingen in webinhoud, zodat de worm de webpagina's kan wijzigen om zich naar andere servers te kunnen verspreiden.

Cisco IDS voldoet aan de standaardbest practices om webservers te beschermen tegen NIMD. Deze optimale werkwijzen dicteren niet om e-mail te lezen of het web van een productieWebserver te bladeren zowel als hebben geen netwerkaandelen open op een server. Cisco IDS Host Sensor voorkomt dat de webserver gecompromitteerd wordt door HTTP en IS-explosies. De bovengenoemde beste praktijken zorgen ervoor dat de Nimda-worm niet met handmatige middelen op de webserver aankomt.

Cisco IDS-netwerksensor (NIMD)

Cisco IDS-netwerksensor identificeert aanvallen voor webtoepassingen, waaronder aanvallen die door de NIMDH-worm worden gebruikt. De netwerksensor is in staat om aanvallen te identificeren en details over de getroffen of gecompromitteerde hosts te verstrekken om de infectie met Nimda te isoleren.

Deze Cisco IDS-netwerksensor vuurt:

- Toegang tot WW WinNT cmd.exe (SigID 5081)
- IS CGI dubbele decode (SigID 5124)
- WWO-aanval met Unicode (SigID 5114)

- IS Dot Execute Attack (SigID 3215)
- IS-aanval op dot-stok (SigID 3216)

De exploitanten zien geen alarm dat Nimda bij naam identificeert. Ze zien een reeks van alarm die wordt geslagen terwijl Nimda verschillende explosies inzet om het doel te bereiken. Het alarm identificeert het bronadres van hosts die gecompromitteerd zijn en die moet worden geïsoleerd van het netwerk, gereinigd en geplakt.

Aanbevolen actieprogramma

Volg deze stappen om te beschermen tegen de Nimda-worm:

1. Pas de nieuwste updates voor Microsoft Outlook, Outlook Express, Internet Explorer en is beschikbaar vanuit Microsoft .
2. update uw virusscansoftware met de nieuwste pleister om de verspreiding van het virus te beperken.**Opmerking:** U kunt de nieuwste viruspleister downloaden om uw pc tegen infectie te beschermen. Als uw pc al is geïnfecteerd, kunt u met deze viruspleister handmatig de harde schijf van uw pc scannen en de infectie van de machine reinigen.
3. IMPLEMENTEER Cisco IDS om de dreiging te beperken, de infectie te beheersen en de servers te beschermen.

Gerelateerde informatie

- Uw netwerk beschermen tegen het NIMA-virus
- Cisco-productbeveiligingsAdvisories en -kennisgevingen
- Ondersteuning van Cisco Secure Inbraakdetectiesysteem
- Technische ondersteuning - Cisco-systemen