Réponse de Cisco Secure IDS au virus Nimda

Contenu

Introduction

Ce document explique comment le système de détection d'intrusion Cisco Secure (ID) l'identifie et empêche la compromission de web server des attaques par le ver Nimda (également connu sous le nom de virus de concept). Le fonctionnement technique complexe du ver est hors de portée de ce bulletin et est bien documenté ailleurs. Une des meilleures descriptions techniques du ver Nimda peut être trouvée dans le ver Nimda CA-2001-26 consultatif CERT® .

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le ver Nimda est un ver et un virus hybrides qui se propage agressivement sur l'Internet. Pour comprendre Nimda et les capacités des ID de Cisco d'atténuer son étalement, il est important de

définir ces deux termes :

- **Le ver** se rapporte au code malveillant qui des étalements automatiquement, sans intervention humaine.
- **Le virus** se rapporte au code malveillant qui se propage par un certain type d'intervention humaine, comme quand vous ouvrez un courrier électronique, parcourent un site Web infecté, ou exécutent manuellement un fichier infecté.

Le ver Nimda est réellement un hybride qui montre des caractéristiques d'un ver et d'un virus. Nimda infecte de plusieurs manières, les la plupart dont exigez l'intervention humaine. Les ID de Cisco hébergent les méthodes comme un ver d'infection de blocs de capteur qui se propagent par des vulnérabilités dans l'Internet Information Server de Microsoft (IIS). Les ID de Cisco ne bloque pas les méthodes de type viral et manuelles d'infection, comme quand vous ouvrez une connexion de courrier électronique, parcourent un site Web infecté, ou exécutez manuellement un fichier infecté.

Le capteur d'hôte d'ID de Cisco se protège contre Nimda

Le capteur d'hôte d'ID de Cisco empêche les attaques de traversée de répertoire, qui incluent ceux utilisés par le ver Nimda. Quand les tentatives de ver de compromettre Cisco Id-ont protégé le web server, l'attaque échoue et le serveur n'est pas compromis.

Ces règles de capteur d'hôte d'ID de Cisco empêchent le succès du ver Nimda :

- Traversée de répertoire IIS (quatre règles)
- Traversée de répertoire IIS et exécution de code (quatre règles)
- Double traversée de répertoire de codage hexadécimal IIS (quatre règles)

Le capteur d'hôte d'ID de Cisco défend également contre les modifications non autorisées au contenu Web, ainsi il ne permet pas au ver de modifier des pages Web afin de se propager à d'autres serveurs.

Les ID de Cisco se conforme aux pratiques recommandées standard de Sécurité de protéger des web server contre Nimda. Ces pratiques recommandées dictent pour ne pas lire le courrier électronique ou pour parcourir le Web d'un web server de production, aussi bien que ne pas avoir des parts du réseau ouvrez-vous sur un serveur. Le capteur d'hôte d'ID de Cisco empêche le web server d'être compromis par des exploits de HTTP et IIS. Les pratiques recommandées mentionnées ci-dessus s'assurent que le ver Nimda n'arrive pas sur le web server par quelques moyens manuels.

Le capteur de réseau d'ID de Cisco identifie Nimda

Le capteur de réseau d'ID de Cisco identifie les attaques d'application Web, qui incluent ceux utilisés par le ver Nimda. Le capteur de réseau peut identifier des attaques et fournir des détails au sujet des hôtes affectés ou compromis pour isoler l'infection de Nimda.

Le feu de ces de Cisco d'ID de réseau alarmes de capteur :

- WWW WinNT cmd.exe Access (SigID 5081)
- Le double CGI IIS décodent (SigID 5124)
- Attaque de WWW IIS Unicode (SigID 5114)

- IIS point-point exécutent l'attaque (SigID 3215)
- Attaque point-point de crash IIS (SigID 3216)

Les opérateurs ne voient pas une alarme qui identifie Nimda de nom. Ils voient une gamme des alarmes remarquables en tant qu'exploits d'essais de Nimda différentes pour compromettre la cible. Les alarmes identifient l'adresse source des hôtes qui ont été compromis et qui devraient être isolés dans le réseau, être nettoyés, et corrigés.

Lignes de conduite recommandée

Suivez ces étapes pour se protéger contre le ver Nimda :

1. Appliquez les dernières mises à jour pour Microsoft Outlook, Outlook Express, l'Internet Explorer, et l'IIS disponible à partir de Microsoft .
2. Mettez à jour votre logiciel de détection de virus avec le dernier correctif pour atténuer l'étalement du virus.**Remarque:** Vous pouvez télécharger le dernier correctif de virus pour protéger votre PC contre l'infection. Si votre PC a été déjà infecté, ce correctif de virus te permet pour balayer manuellement le disque dur de votre PC et pour nettoyer l'infection de l'ordinateur.
3. Déployez les ID de Cisco pour atténuer la menace, contenez l'infection, et protégez les serveurs.

Informations connexes

- Comment protéger votre réseau contre le virus Nimda
- Notifications et conseils de sécurité au sujet des produits Cisco
- Page Cisco Secure de prise en charge de la détection d'intrusion
- Support technique - Cisco Systems