Utilisation de signatures de correspondance de chaîne personnalisée Cisco Secure IDS/NetRanger pour débordement de mémoire tampon distant de ver « Code Red » dans l'extension ISAPI de Microsoft Index Server, dans IIS 4.0 et 5.0

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Signatures de correspondance de chaîne personnalisée
Signature 1 — Serveur d'index Access avec l'exploitation tentée
Signature 2 — Ver de « Code Red » de Buffer Overflow d'Access de serveur d'index
Informations connexes

Introduction

Àpartir de fin juillet 2003, l'économie d'ordinateur (une organisation pour la recherche indépendante à Carlsbad, CA) a estimé que le ver de « Code Red » avait coûté à des sociétés $1.2 milliards (les États-Unis) dans la reprise des dommages de réseau et dans la perte de productivité. Cette évaluation a monté de manière significative avec la version suivante du ver plus efficace du « Code Red II ». Le système de détection d'intrusion Cisco Secure (ID), un élément clé du plan détaillé SÛR de Cisco, a expliqué sa valeur en détectant et des risques de sécurité des réseaux d'atténuation, y compris le ver de « Code Red ».

Ce document décrit une mise à jour logicielle pour détecter la méthode d'exploitation utilisée par le ver de « Code Red » (voir la signature 2 ci-dessous).

Vous pouvez créer les signatures de correspondance de chaîne personnalisée affichées ci-dessous pour attraper l'exploitation d'un débordement de tampon pour des web server exécutant le NT de Microsoft Windows et l'Internet Information Services (IIS) 4.0 ou Windows 2000 et IIS 5.0. Notez également que le service d'indexation dans Windows XP bêta est également vulnérable. Le bulletin de renseignements de Sécurité qui décrit cette vulnérabilité est chez http://www.eeye.com/html/Research/Advisories/AD20010618.html . Microsoft a libéré un correctif pour cette vulnérabilité qui peut être téléchargée de http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx .

Les signatures discutées dans ce document sont devenues disponibles dans la version de mise à jour de signature S(5). Cisco Systems recommande que des capteurs soient mis à jour à 2.2.1.8 ou à la mise à jour de la signature 2.5(1)S3 avant de mettre en application cette signature. Les utilisateurs enregistrés peuvent télécharger ces mises à jour de signature du centre Cisco Secure de logiciel. Tous les utilisateurs peuvent entrer en contact avec le support technique de Cisco par le courrier électronique et le téléphone par les Cisco Worldwide Contacts.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel suivantes :

- NT et IIS 4.0 de Microsoft Windows
- Microsoft Windows 2000 et IIS 5.0

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Signatures de correspondance de chaîne personnalisée

Il y a deux signatures de correspondance de chaîne personnalisée spécifiques pour aborder cette question. Chaque signature est décrite ci-dessous, et des configurations applicables de produit sont fournies.

Signature 1 — Serveur d'index Access avec l'exploitation tentée

Cette signature se déclenche sur un débordement de tampon tenté sur l'extension ISAPI du serveur d'indexation combinée avec une tentative de passer le code de shell au serveur pour gagner l'accès privilégié sous la grille d'origine du code. Les feux de signature seulement sur la tentative de passer le code de shell au service de destination afin d'essayer de gagner le plein accès au niveau système. Un problème éventuel est que cette signature ne se déclenche pas si l'attaquant n'essaye pas de ne passer aucun code de shell, mais exécute juste le débordement de tampon contre le service afin d'essayer de tomber en panne IIS et créer un déni de service.

Chaîne

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Configurations de produit

- Occurrences : 1
- Port : 80

Remarque: Si vous avez des web server écoutant sur d'autres ports TCP (par exemple, 8080), vous devez créer une concordance de la chaîne personnalisée distincte pour chaque numéro de port.

- Niveau recommandé de sévérité d'alarme :Haute (Cisco Secure Policy Manager)5 (directeur d'Unix)
- Direction :À

Signature 2 — Ver de « Code Red » de Buffer Overflow d'Access de serveur d'index

Les deuxièmes feux de signature sur un débordement de tampon tenté sur l'extension ISAPI du serveur d'indexation combinée avec une tentative de passer le code de shell au serveur pour gagner l'accès privilégié sous la forme assombrie que le ver de « Code Red » utilise. Cette signature se déclenche seulement sur la tentative de passer le code de shell au service de destination afin d'essayer de gagner le plein accès au niveau système. Un problème éventuel est que cette signature ne se déclenche pas si l'attaquant n'essaye pas de ne passer aucun code de shell, mais exécute juste le débordement de tampon contre le service afin d'essayer de tomber en panne IIS et créer un déni de service.

Chaîne

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Remarque: Il n'y a aucun espace dans la chaîne ci-dessus.

Configurations de produit

- Occurrences : 1
- Port : 80

Remarque: Si vous avez des web server écoutant sur d'autres ports TCP (par exemple, 8080), vous devez créer une concordance de la chaîne personnalisée distincte pour chaque numéro de port.

- Niveau recommandé de sévérité d'alarme :Haute (Cisco Secure Policy Manager)5 (directeur d'Unix)
- Direction :À

Pour plus d'informations sur le Cisco Secure IDS, référez-vous à la détection Cisco Secure d'intrusion.

Informations connexes

- Soutien technique – Routeurs
- Avis de sécurité Cisco
- Page Cisco Secure de prise en charge de la détection d'intrusion

- Support technique - Cisco Systems