Comment filtrer Code Red sur le cache Cisco et les modules Content Engine

Contenu

Introduction

Ce document fournit des informations sur filtrer le ver Code Red sur des engines de cache et de contenu de Cisco.

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.

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.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Configurations

Beaucoup de caches transparents sont accablés en tentant de se connecter aux sites inexistants. Ce document fournit une solution pour filtrer le ver Code Red qui peut affecter Cisco cachant des solutions. Le Code Red utilise une exploit de débordement de tampon dans un script default.ida sur les Internets Information Server (IIS). Le Code Red utilise cette demande de Protocole HTTP (Hypertext Transfer Protocol) :

```
get http://random-ip-address/default.ida?long-string-of-data
```

`Les long-chaîne-de-données de l'`exemple ci-dessus sont le code de débordement de tampon et d'instruction pour le ver lui-même. Vous pouvez filtrer ceci à l'aide d'une règle de bloc qui emploie une URL-expression régulière pour apparier le contenu. Pour le matériel de moteur de cache de Cisco exécutant le logiciel CE2.XX, et le matériel de Cisco Content Engine exécutant le logiciel 2.XX ou 3.XX, configurez comme suit :

```
rule enable
rule block url-regex ^http://.*/default\.ida$
rule block url-regex ^http://.*www\.worm\.com/default\.ida$
```

Émettez la **règle d'exposition toute la** commande d'afficher le nombre de hits qui s'accumulent contre cette règle de bloc. Pour le matériel satisfait d'engine exécutant le logiciel 3.XX, vous pouvez être plus de particularité et ne pas bloquer la demande, mais réécriture à un serveur Web local d'indiquer que votre site est infecté. Utilisez une règle semblable à celle-ci :

```
rule enable
rule rewrite url-regsub ^http://.*/default\.ida$ http://local-webserver/codered.html
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support produit de Réseau de diffusion de contenu
- Téléchargements logiciels du moteur de cache 3.0 de Cisco (clients enregistrés seulement)
- Téléchargements logiciels du moteur de cache 2.0 de Cisco (clients enregistrés seulement)
- Support technique - Cisco Systems