Acción de advertencia de acceso seguro de Cisco Anular comportamiento con configuración de bloqueo IPS

Contenido

Problema

Al probar el comportamiento de advertencia en una política de acceso (acceso a Internet) en Cisco Secure Access con IPS activado, los usuarios experimentan un comportamiento inesperado en el que la acción de advertencia aparece para anular la configuración de bloqueo IPS. Específicamente, cuando se accede a una URL destinada a activar una firma IPS (intento de acceso a un archivo SERVER-WEBAPP /etc/passwd, GID-SID: 1-1122), se muestra una página de advertencia y, tras la confirmación del usuario, se permite el acceso a la URL a pesar de que IPS se haya configurado para bloquear el tráfico.

La configuración incluye:

- Acción: Aislar
- Prevención de intrusiones (IPS): Habilitar
- IPS/Bloquear
- Firma: Intento de acceso al archivo SERVER-WEBAPP /etc/passwd
- GID-SID: 1-1122

Los registros de búsqueda de actividad muestran entradas conflictivas:

- IPS: (IPS: bloqueo)
- WEB: (WEB: permitir: se muestra una página de advertencia)
- WEB: (WEB: permitir (tras el acceso de advertencia)

Entorno

- Producto: Ventaja de Cisco Secure Internet Access
- Tecnología: Acceso seguro
- Política de acceso configurada con la acción Acceso a Internet y Avisar
- IPS habilitado con acción de bloqueo para firmas específicas

Resolución

Este comportamiento se ha identificado como un defecto en Cisco Secure Access, donde la acción Advertir de las políticas de acceso tiene prioridad sobre la configuración de bloqueo IPS. Este problema afecta a la interacción entre las acciones de advertencia de la política de acceso y la funcionalidad de bloqueo IPS.

Pasos de verificación

Para verificar este comportamiento en su entorno:

Paso 1: Configuración de la política de acceso con la acción de advertencia y activación del bloqueo IPS

- Establecer acción para aislar con comportamiento de advertencia
- Habilitar la prevención de intrusiones (IPS)
- Configurar IPS con acción Bloquear
- Aplique una firma específica (p. ej., intento de acceso al archivo SERVER-WEBAPP /etc/passwd, GID-SID: 1-1122)

Paso 2: Pruebe la configuración accediendo a una URL que activa la firma IPS

```
https://example.com/etc/passwd
```

Paso 3: Observar el comportamiento

- Se mostrará una página de advertencia al usuario
- El usuario puede continuar después de confirmar la advertencia
- Se permitirá el acceso a la URL a pesar de la configuración del bloque IPS

Paso 4: Comprobar registros de búsqueda de actividad

- Verificar la presencia de entradas de bloqueo IPS y de permiso WEB
- Confirme que las entradas de registro en conflicto indiquen el defecto

Estado actual

Este comportamiento se ha confirmado como un defecto en el que la acción Advertir anula la configuración de bloqueo IPS por diseño en la implementación actual. El mismo comportamiento ocurre con las firmas IPS que no son GID-SID: 1-1122, lo que indica que se trata de un problema sistémico que afecta a todas las firmas IPS cuando se configuran acciones de advertencia.

Aún no se ha determinado un plan de corrección y un calendario para este defecto. Las organizaciones que experimenten este problema deben evaluar sus políticas de seguridad y considerar configuraciones alternativas si se requiere un bloqueo IPS estricto.

Causa

La causa principal es un defecto en Cisco Secure Access, donde el procesamiento de la acción de advertencia de la política de acceso tiene prioridad sobre la aplicación del bloque IPS. Este defecto de diseño permite a los usuarios omitir los controles de seguridad IPS a través del mecanismo de confirmación de advertencia, anulando de forma efectiva la funcionalidad de bloqueo IPS cuando se configuran las acciones de advertencia.

El ID de bug Cisco CSCwt39270 está asociado con este caso, aunque la relación específica entre este bug y el comportamiento observado de advertir versus IPS requiere una investigación más detallada.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).