Resolución de problemas de eventos de intrusión de FMC que muestran impacto=Desconocido

Contenido

Problema

Después de implementar un nuevo Firewall Management Center (FMC) y actualizar a la versión 7.7.12, todos los eventos de intrusión muestran "Impact=Unknown" en lugar de los valores de impacto esperados. Esto evita que se activen los mecanismos de alerta adecuados, ya que el campo de impacto es necesario para la configuración de alertas.

Entorno

- FMC versión 7.7.12. Otras versiones de software también pueden verse afectadas.
- Directiva de intrusiones en modo de prevención o detección.

Resolución

La resolución de este problema implica verificar y configurar el alcance de la política de detección para incluir todas las direcciones IP relevantes donde se generan los eventos de intrusión.

Paso 1. Identificar las direcciones IP afectadas

Revise los eventos de intrusión que muestran "Impact=Unknown" e identifique las direcciones IP

específicas involucradas en estos eventos. Documente estas direcciones IP para compararlas con la configuración actual de la política de detección.

Paso 2. Revisar la configuración actual de la directiva de detección

Navegue hasta Políticas de FMC > Detección de red (en las versiones más recientes es Políticas > Avanzado > Detección de red) y examine la configuración actual de la política de detección para determinar qué rangos de direcciones IP o subredes están incluidos actualmente en el alcance de detección.

Paso 3. Actualizar ámbito de directiva de descubrimiento

Modifique la configuración de la directiva de detección para incluir todas las direcciones IP en las que se producen eventos de intrusión. Asegúrese de que el ámbito de la política de detección abarca todos los segmentos de red en los que espera recibir eventos de intrusión con una evaluación de impacto adecuada.

Paso 4. Implementación de cambios de configuración

Implemente la configuración de la directiva de detección actualizada en todos los dispositivos administrados para garantizar que los cambios surtan efecto en toda la infraestructura de seguridad.

Paso 5. Verificar la cumplimentación del campo de impacto

Supervise los nuevos eventos de intrusión para confirmar que el campo de impacto se está rellenando con los valores adecuados en lugar de "Desconocido".

Causa

Los eventos de intrusión que muestran "Impact=Unknown" se debieron a un problema de configuración en el que las direcciones IP afectadas no se incluyeron en ninguna política de detección de FMC. Cuando las direcciones IP quedan fuera del ámbito de las políticas de detección configuradas, el FMC no puede evaluar correctamente el impacto de los eventos de intrusión para esas direcciones, lo que hace que el campo de impacto se rellene con valores "Desconocido". Se trata de un problema relacionado con la configuración en lugar de un defecto de software o hardware.

Contenido relacionado

- Niveles de impacto de eventos de intrusión
- 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).