

Actualización del motor Snort bloqueada durante la actualización de FTD debido a la detección de políticas personalizadas

Contenido

Problema

Durante una actualización de FTD de la versión 7.2 a la 7.4.4 en un HA FPR-4115 gestionado por FMC, la actualización del motor Snort a Snort 3 se bloquea con mensajes de error que indican un fallo a la hora de convertir las reglas personalizadas de Snort 2 o el uso de intrusiones personalizadas o políticas de análisis de red. El mensaje de error específico indica: "No se puede actualizar a Snort 3. El dispositivo utiliza al menos una política de intrusiones personalizada o una política de análisis de red." Un mensaje de fallo más detallado indica que no se pueden convertir las reglas personalizadas de Snort 2 y apunta a `/var/sf/htdocs/ips/snort.rej` para obtener más información. La cuestión es si este error impediría la migración a Snort 3 y afectaría a la funcionalidad de inspección.

Entorno

- Cisco Secure Firewall Firepower versión 7.3
- Firepower Management Center (FMC) versión 7.7.11
- Dispositivos FTD en configuración de alta disponibilidad (HA)
- Hardware FPR-4115
- Ruta de actualización: FTD 7.2 a 7.4.4
- La última versión de VDB antes de la actualización
- La sección Reglas locales de Objetos > Reglas de intrusión > Snort 2 Todas las reglas está vacía

Resolución

El mensaje de error que bloquea la actualización del motor Snort es un comportamiento documentado relacionado con el ID de bug Cisco CSCwn46794 y no representa un bloqueador funcional cuando no existen reglas de Snort 2 personalizadas.

Pasos de verificación

Paso 1: Verificar el estado de las reglas del Snort 2 personalizado

Vaya a la interfaz de FMC y compruebe si hay reglas de Snort 2 personalizadas:

Paso 2: Confirmar la versión de VDB

Asegúrese de que la base de datos de vulnerabilidades (VDB) tiene la última versión antes de continuar con la actualización.

Paso 3: Revisar los detalles del error

Verifique la información de error detallada en el archivo al que se hace referencia:

```
/var/sf/htdocs/ips/snort.rej
```

Proceso de actualización

Cuando se confirma que la sección "Local Rules" (Reglas locales) está vacía (no hay reglas Snort 2 personalizadas presentes), la actualización puede continuar a pesar del mensaje de error. El error de bloqueo es un falso positivo en este escenario y no indica reglas personalizadas reales que necesiten conversión.

Paso 1: Continúe con la actualización de Snort 3

Continúe con el proceso de actualización de FTD a la versión 7.4.4, que incluye la actualización del motor Snort 3.

Paso 2: Validación posterior a la actualización

Una vez que la actualización se haya completado correctamente, pruebe el flujo de tráfico para confirmar el comportamiento esperado con el motor Snort 3.

Paso 3: Supervisar el rendimiento del sistema

Valide que la funcionalidad de inspección funciona según lo previsto con el nuevo motor Snort 3.

Causa

El mensaje de bloqueo de actualización es un comportamiento documentado asociado con el Id. de error de Cisco CSCwn46794. Este error hace que el sistema muestre un mensaje de error sobre las políticas de intrusión personalizadas o las políticas de análisis de red incluso cuando no existen reglas de Snort 2 personalizadas que requieran conversión. El mensaje de error aparece como un falso positivo cuando la sección de reglas locales está vacía, pero la validación previa a la actualización del sistema identifica incorrectamente la presencia de políticas personalizadas.

Contenido relacionado

- [ID de bug de Cisco CSCwn46794](#)

- [ID de bug de Cisco CSCwk07199](#)
- [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).