Aclare el proceso de actualización de VDB en FMC

Contenido

Problema

Al ejecutar actualizaciones de base de datos de vulnerabilidades (VDB), los administradores deben saber si las actualizaciones de VDB son acumulativas y si pueden omitir versiones intermedias.

En este ejemplo, la preocupación es cuando se actualiza desde la versión 393 de VDB a la versión 427. Específicamente, hay incertidumbre sobre si se requieren varios pasos de actualización o si se admite una ruta de actualización directa. Además, surgen preocupaciones sobre las posibles interrupciones del servicio durante la actualización de la VDB y el posterior proceso de implementación de políticas.

Entorno

- Versión 7.4.2.4 del software Secure Firewall Management Center (FMC). Otras versiones del software también se ven afectadas.
- Firewall Threat Defence (FTD) en FPR 2110. Otras plataformas de hardware también se ven afectadas.
- Versión actual de VDB: 393. Otras versiones de software también se ven afectadas.
- Versión de VDB de destino: 427. Otras versiones de programas informáticos también se ven afectadas.

Resolución

Las actualizaciones de VDB en FMC son acumulativas, lo que permite actualizaciones directas de versiones anteriores a versiones más recientes sin necesidad de pasos intermedios.

Proceso de actualización de VDB

Puede actualizar directamente desde la versión 393 de VDB a la versión 427 de VDB sin ningún paso intermedio de actualización de VDB. A partir de la versión 357 de VDB, Cisco admite la instalación de cualquier versión de VDB desde la base de VDB en la plataforma FMC.

Para descargar la última versión de VDB, vaya al centro de descargas de software de Cisco en https://software.cisco.com/download/home/286332319/type/286321931/release/VDB

Consideraciones sobre el impacto del servicio

El riesgo principal no está asociado con la instalación de la VDB en el FMC, sino con la primera implementación de políticas en el FTD después de la actualización de la VDB. En la mayoría de los casos, la primera implementación después de una actualización de VDB reinicia el proceso Snort, que interrumpe temporalmente la inspección del tráfico.

Durante este período de interrupción:

- El tráfico puede descartarse o pasar sin inspección adicional.
- El comportamiento específico depende de cómo se configure el FTD para manejar el tráfico durante los reinicios del proceso.

Recomendaciones de prácticas recomendadas:

- Programe la parte de implementación de políticas durante un período de mantenimiento planificado.
- Coordine con las operaciones de red para minimizar el impacto en el usuario.
- Supervise el estado del sistema durante y después del proceso de implementación.

Causa

- A partir de VDB 357, puede instalar cualquier actualización de VDB desde la base de VDB para el FMC.
- La instalación requiere una reimplementación de políticas para activar las nuevas firmas de vulnerabilidades, lo que desencadena un reinicio del proceso Snort en los dispositivos FTD administrados. Este reinicio crea una breve interrupción en las capacidades de inspección de tráfico mientras se carga la nueva base de datos y el motor de inspección se reinicializa.

Contenido relacionado

- Guía de administración de Cisco Secure Firewall Management Center: actualizaciones del sistema
- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center: implementación
- 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).