HOT BULLETIN

CA23-03, CA23-04 y CA23-05.

26 abril de 2023

Devel
CYBERSECURITY REDEFINED

- Web: www.devel.group
- Email: info@develsecurity.com
- Guatemala - El Salvador - Honduras - Rep. Dominicana

Contenido

Resumen ejecutivo

Estimado cliente,

CyberArk ha publicado los boletines de seguridad CA23-03, CA23-04 y CA23-05.

CA23-03 implica un cambio identificado recientemente en la configuración de protección de políticas de Chrome que causó un endurecimiento insuficiente de Chrome en la máquina PSM. La vulnerabilidad afecta a todas las versiones de Privilege Cloud Connector anteriores a 12.7 y a todas las versiones autohospedadas de Privileged Session Manager anteriores a la versión 13.0.

A esta vulnerabilidad se le asignó una clasificación **de gravedad alta**.

CA23-04 implica una vulnerabilidad recientemente identificada en Privileged Session Manager (PSM) que puede exponer potencialmente las contraseñas de PSMConnect y PSMAdminConnect, en determinadas configuraciones, durante el proceso de instalación o actualización de PSM. La vulnerabilidad afecta a todas las versiones de Privilege Cloud Connector y a todas las versiones autohospedadas de Privileged Session Manager.

A esta vulnerabilidad se le asignó una clasificación **de gravedad alta**.

CA23-05 implica una vulnerabilidad recientemente identificada en Privileged Session Manager (PSM) que puede causar una denegación de servicio para el servicio PSM al conectarse con ciertos componentes de conexión en determinadas circunstancias. La vulnerabilidad afecta a las versiones 12.5, 12.6, 12.7 y 13.0 de Privilege Cloud Connector, así como a las versiones 12.6 y 13.0 de Privileged Session Manager autohospedadas.

A esta vulnerabilidad se le asignó una clasificación **de gravedad alta**.

Boletín de seguridad de Cyberark CA23-03

Un cambio identificado recientemente en la configuración de endurecimiento de la política de Chrome provocó un endurecimiento insuficiente de Chrome en la máquina PSM.

20-03-2023 • Artículo de conocimiento

Número de artículo:

000030349

Título:

Boletín de seguridad de Cyberark CA23-03

Detalles:

Administrador de acceso de privilegios auto-hospedado: Falta de valores de refuerzo en el GPO de Privileged Session Manager debido a cambios en la política de Chrome

Emitido: 20 de marzo de 2023

Actualizado: NA

Versión: 1.0

Gravedad: Alta

INFORMACIÓN GENERAL

Resumen ejecutivo

Un cambio identificado recientemente en la configuración de endurecimiento de la política de Chrome provocó un endurecimiento insuficiente de Chrome en la máquina PSM.

Software afectado

Todas las versiones de Privileged Session Manager autohospedadas anteriores a la versión 13.0.

Explicación detallada

El uso por parte de versiones autohospedadas de PSM anteriores a la versión 13.0 de valores de protección obsoletos por Chrome, en lugar de los valores actualizados en el GPO proporcionado a Privileged Session Manager, provocó una configuración de protección

insuficiente de Chrome en la máquina PSM. La falta de la configuración ajustada podría permitir que PSM realice operaciones compatibles con Chrome que anteriormente estaban bloqueadas.

Recomendaciones

CyberArk recomienda a todos los clientes que utilicen versiones de Privileged Session Manager autohospedadas anteriores al parche de la versión 13.0 o que actualicen el PSM de acuerdo con las instrucciones a continuación.

INSTRUCCIONES

Actualice su PSM a la versión de parche correspondiente a continuación descargándolo desde el enlace respectivo y siguiendo las instrucciones de actualización correspondientes https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS INST/Upgrading- el-Privileged-Session-Manager.htm.

Ejecute el procedimiento de endurecimiento apropiado para PSM como se describe en la documentación vinculada en la tabla.

Para implementaciones en el dominio, actualice el GPO como se describe en la documentación vinculada en la tabla.

Nota: Los parches de PSM son compatibles con versiones anteriores de PAS que se encuentran dentro de su período de desarrollo, según la política de fin de vida útil de CyberArk.

Versión instalada	Versión de parche	Enlace de descarga	Documentación
11.5	11.5.15	https://www.cyberark.com/PSM-11.5.15	• Instrucciones de actualización 11.5 • Tareas de endurecimiento de PSM • Fortalecimiento de la implementación 'en dominio'
12.2	12.2.10	https://www.cyberark.com/PSM-12.2.10	• 12.2 instrucciones de actualización • Tareas de endurecimiento de PSM

			• Fortalecimiento de la implementación 'en dominio'
12.6	12.6.5	https://www.cyberark.com/PSM-12.6.5	• 12.6 instrucciones de actualización • Tareas de endurecimiento de PSM • Fortalecimiento de la implementación 'en dominio'

Nota: si usa una versión de Chrome anterior a v86 y nunca ha ejecutado la configuración de protección de GPO, la versión de Chrome debe actualizarse antes de aplicar el parche de PSM.

PREGUNTAS FRECUENTES (FAQ)

¿Esta vulnerabilidad pone en riesgo el servidor Vault?

No, esta vulnerabilidad solo afecta a Privileged Session Manager.

¿Puede esta vulnerabilidad ser aprovechada por cualquier usuario?

Cualquier usuario autenticado que pueda conectarse usando Chrome a través de PSM puede aprovechar esta vulnerabilidad. Un usuario no autenticado puede aprovechar esta vulnerabilidad si un usuario autenticado ha instalado una extensión maliciosa de Chrome.

¿Existe un exploit público para esta vulnerabilidad?

CyberArk no ha recibido ninguna información que indique que esta vulnerabilidad haya sido explotada en ningún entorno de cliente.

Boletín de seguridad de Cyberark CA23-04

Una vulnerabilidad identificada recientemente en Privileged Session Manager (PSM) puede potencialmente exponer las contraseñas de PSMConnect y PSMAdminConnect, en ciertas configuraciones, durante el proceso de instalación o actualización de PSM.

20-03-2023 • Artículo de conocimiento

Número de artículo:

000030351

Título:

Boletín de seguridad de Cyberark CA23-04

Detalles:

Privilege Access Manager auto-hospedado: posible exposición de datos confidenciales en Privileged Session Manager

Emitido: 20 de marzo de 2023

Actualizado: NA

Versión: 1.0

Gravedad: Alta

INFORMACIÓN GENERAL
Resumen ejecutivo

Una vulnerabilidad identificada recientemente en Privileged Session Manager (PSM) puede potencialmente exponer las contraseñas de PSMConnect y PSMAdminConnect, en ciertas configuraciones, durante el proceso de instalación o actualización de PSM.

Software afectado

Todas las versiones de Privileged Session Manager autohospedadas.

Explicación detallada

Bajo ciertas configuraciones de auditoría, las contraseñas de PSMConnect y PSMAdminConnect pueden estar expuestas en el registro de eventos de Windows durante la instalación o actualización de PSM. Si hay integración del sistema SIEM, las contraseñas pueden enviarse a un sistema externo.

Recomendaciones

CyberArk recomienda encarecidamente que todos los clientes que utilicen versiones de Privileged Session Manager autohospedadas parcheen o actualicen el PSM de acuerdo con las instrucciones a continuación.

Debido a la confidencialidad de las credenciales de PSMConnect y PSMAdminConnect, CyberArk recomienda enfáticamente, como mejor práctica de seguridad, que estas credenciales sean administradas por CPM. Asocie una cuenta de conciliación con la plataforma para garantizar una rotación de contraseñas exitosa. Para obtener más información, consulte Configurar las contraseñas de los usuarios de PSM.

INSTRUCCIONES

Actualice su PSM a la versión de parche correspondiente a continuación descargándolo desde el enlace respectivo y siguiendo las instrucciones de actualización correspondientes https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS INST/Upgrading- el-Privileged-Session-Manager.htm

Nota: Los parches de PSM son compatibles con versiones anteriores de PAS que se encuentran dentro de su período de desarrollo, según la política de fin de vida útil de CyberArk.

Versión instalada	Versión de parche	Enlace de descarga	Documentación
11.5	11.5.15	https://www.cyberark.com/PSM-11.5.15	Instrucciones de actualización 11.5
12.2	12.2.10	https://www.cyberark.com/PSM-12.2.10	12.2 instrucciones de actualización
12.6	12.6.5	https://www.cyberark.com/PSM-12.6.5	12.6 instrucciones de actualización
13.0	13.0.1.	https://www.cyberark.com/PSM-13.0.1	Instrucciones de actualización 13.0

PREGUNTAS FRECUENTES (FAQ)

¿Esta vulnerabilidad pone en riesgo el servidor Vault?

No, esta vulnerabilidad solo afecta a Privileged Session Manager.

¿Puede esta vulnerabilidad ser aprovechada por cualquier usuario?

Cualquier usuario que tenga privilegios para ver los registros de eventos en el servidor PSM o, con la integración del sistema SIEM, tiene privilegios para ver los registros en el sistema SIEM, puede ver los datos confidenciales.

¿Existe un exploit público para esta vulnerabilidad?

CyberArk no ha recibido ninguna información que indique que esta vulnerabilidad haya sido explotada en ningún entorno de cliente.

Boletín de seguridad de Cyberark CA23-05

Una vulnerabilidad recientemente identificada en Privileged Session Manager (PSM) puede potencialmente causar una denegación de servicio para el servicio PSM cuando se conecta con ciertos componentes de conexión en ciertas circunstancias.

20-03-2023 • Artículo de conocimiento

Número de artículo:

000030353

Título:

Boletín de seguridad de Cyberark CA23-05

Detalles:

Administrador de acceso privilegiado autohospedado: posible denegación de servicio (DoS) del administrador de sesión privilegiado

Emitido: 20 de marzo de 2023

Actualizado: NA

Versión: 1.0

Gravedad: Alta

INFORMACIÓN GENERAL

Resumen ejecutivo

Una vulnerabilidad recientemente identificada en Privileged Session Manager (PSM) puede potencialmente causar una denegación de servicio para el servicio PSM cuando se conecta con ciertos componentes de conexión en ciertas circunstancias.

Software afectado

Privileged Session Manager autohospedado versiones 12.6 y 13.0.

Explicación detallada

La conexión a través de PSM utilizando ciertos componentes de conexión que contienen cierta entrada manipulada puede dar lugar a una denegación de servicio de PSM.

Recomendaciones

CyberArk recomienda encarecidamente que todos los clientes que utilicen las versiones 12.6 y 13.0 de Privileged Session Manager autohospedadas parcheen o actualicen el PSM de acuerdo con las instrucciones a continuación.

INSTRUCCIONES

Actualice su PSM a la versión de parche correspondiente a continuación descargándolo desde el enlace respectivo y siguiendo las instrucciones de actualización correspondientes https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS INST/Upgrading- el-Privileged-Session-Manager.htm.

Nota: Los parches de PSM son compatibles con versiones anteriores de PAS que se encuentran dentro de su período de desarrollo, según la política de fin de vida útil de CyberArk.

Versión instalada	Versión de parche	Enlace de descarga	Documentación
12.6	12.6.5	https://www.cyberark.com/PSM-12.6.5	12.6 instrucciones de actualización
13.0	13.0.1.	https://www.cyberark.com/PSM-13.0.1	Instrucciones de actualización 13.0

PREGUNTAS FRECUENTES (FAQ)

¿Esta vulnerabilidad pone en riesgo el servidor Vault?

No, esta vulnerabilidad solo afecta a Privileged Session Manager.

¿Puede esta vulnerabilidad ser aprovechada por cualquier usuario?

Un usuario malicioso autenticado en PVWA puede explotar el problema.

¿Existe un exploit público para esta vulnerabilidad?

CyberArk no ha recibido ninguna información que indique que esta vulnerabilidad haya sido explotada en ningún entorno de cliente.

Por favor comunícate con nosotros a soporte@develsecurity.com ante cualquier soporte, reporte de amenaza o cualquier otro incidente sobre este boletín de seguridad.