Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

# VULNERABILIDAD EN CYBERARK PASSWORD VAULT WEB ACCESS (PVWA): CVE-2024-38996

*27/ 08 / 2025*

# CONTENIDO

## INTRODUCCIÓN

CyberArk publicó recientemente un nuevo boletín de seguridad (CA25-29) alertando sobre una vulnerabilidad de severidad alta que afecta a Password Vault Web Access (PVWA). Este es el portal web utilizado para acceder a credenciales privilegiadas en entornos corporativos.

## VULNERABILIDAD EN CYBERARK PASSWORD VAULT WEB ACCESS (PVWA): CVE-2024-38996

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|---|---|
| **ID de alerta:** | DSOC-CERT_2025_08_27_2 |
| **Clasificación de alerta:** | Noticia |
| **Tipo de Impacto:** | Alta |
| **TLP (Clasificación de información):** | **CLEAR** |
| **Fecha de publicación:** | 27/08/2025 |
| **Es día cero (0 day):** | No |

## RESUMEN

CyberArk publicó recientemente un nuevo boletín de seguridad (CA25-29) alertando sobre una vulnerabilidad de severidad alta que afecta a Password Vault Web Access (PVWA). Este es el portal web utilizado para acceder a credenciales privilegiadas en entornos corporativos.

La vulnerabilidad, identificada con el CVE-2025-38996, tiene una puntuación CVSS de 7.8 y está relacionada con un problema de Prototype Pollution, un tipo de ataque que puede modificar objetos internos de una aplicación y abrir la puerta a comportamientos inesperados o la ejecución de acciones no autorizadas.

### Productos y versiones afectadas

La vulnerabilidad afecta a todas las versiones de PVWA Self-Hosted anteriores a las siguientes:

- Versión 14.2.4
- Versión 14.0.6

Para los clientes de PAM On Cloud:

- Las versiones 14.2 y posteriores deben actualizarse a la imagen corregida en AWS (v14.2.15) o Azure (v14.2.15).
- Las versiones anteriores a la 14.2 deben aplicar las mismas actualizaciones que los entornos locales.

### ¿Qué es el Prototype Pollution?

Para entender esta vulnerabilidad, es importante comprender que en entornos de JavaScript o Node.js, los objetos tienen una "base" llamada prototype.

Si un cibercriminal logra inyectar propiedades maliciosas en ese prototype, todos los objetos que lo utilicen heredarán esas propiedades. Esto puede alterar el funcionamiento normal de la aplicación y abrir la puerta a ataques más serios, como la ejecución de código, el escalamiento de privilegios o la elusión de controles de seguridad.

### ¿Cómo funciona el ataque?

Aunque no se ha reportado ninguna Prueba de Concepto (PoC) activa, la lógica del ataque sería la siguiente:

1. El cibercriminal encuentra una función de entrada de datos mal validada en PVWA, como parámetros JSON que se procesan sin restricciones.
2. Envía una carga maliciosa (payload) que agrega nuevas propiedades al prototype global. Por ejemplo: {"__proto__": {"isAdmin": true}}.

3. Cuando la aplicación crea nuevos objetos, automáticamente heredan esa propiedad. Si algún flujo de validación depende de esta propiedad (if(user.isAdmin)), el cibercriminal puede elevar sus privilegios o modificar comportamientos críticos.

En un sistema como PVWA, esto es especialmente grave porque el software gestiona credenciales privilegiadas. Un cibercriminal podría intentar obtener acceso indebido a cofres de contraseñas, manipular procesos de autenticación o provocar fallas de disponibilidad.

**¿Por qué es importante esta vulnerabilidad?**

PVWA es la puerta de entrada web a cuentas privilegiadas. Si un cibercriminal lograra explotar esta vulnerabilidad, podría:

- Manipular el comportamiento del sistema sin necesidad de romper las credenciales directamente.
- Exponer información confidencial como contraseñas, llaves SSH o cuentas de servicio.

Por ahora, no se ha reportado una explotación activa en la práctica. **Se puede coordinar la mitigación a tac@devel.group**

## RECOMENDACIONES

- Actualiza inmediatamente a las versiones parcheadas:
  - Si usas PVWA 14.2 (LTS) o versiones con parches anteriores a 14.2.4, actualiza a la 14.2.4.
  - Si usas PVWA 14.0 (LTS) o versiones con parches anteriores a 14.0.6, actualiza a la 14.0.6.
- Para clientes de PAM On Cloud:
  - Si usas la versión 14.2 o posterior, despliega la imagen parcheada en AWS (v14.2.15) o Azure (v14.2.15).
  - Si usas versiones anteriores a 14.2, aplica las mismas actualizaciones que los entornos locales.

## NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-en-cyberark-password-vault-web-access-pvwa-cve-2024-38996/

# CONTACTOS DE SOPORTE


**Correo electrónico:** cti@develsecurity.com

**Teléfonos directos:**

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

**Sitio Web:** https://devel.group