Boletín de alerta

Boletín Nro.: 68
Fecha de publicación: 08/07/2026
Tema: Alerta 2026-68 Vulnerabilidades importantes en Idira
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas
EPM SaaS Windows Agent	Todas las versiones anteriores a 26.6
EPM SaaS Windows Agent	Todas las versiones anteriores a 26.6
Privileged Threat Analytics (PTA) / PAM Self□Hosted	Todas las versiones anteriores a 15.2
Vault / Infra Self□Hosted	Todas las versiones anteriores a 15.0.3 (inclusive)
Remote Control Client	Todas las versiones anteriores a 15.0.3 (inclusive)

Descripción

Se han reportado 5 vulnerabilidades importantes en Idira (anteriormente CyberArk, ahora parte de Palo Alto Networks) que afectan componentes clave de su stack de privilegios: agentes de Endpoint Privilege Manager (EPM), la plataforma de analítica PTA/PAM Self□Hosted, el Vault/Infra y el Remote Control Client. Actualmente, de los cinco, únicamente **CA26□27** tiene CVE público asignado: **CVE□2026□22016** (CVSS v4.0: **8.7**), correspondiente a una divulgación de información en el componente de terceros Azul Zulu/JAXP utilizado por Privileged Threat Analytics.

Dado que Idira es la plataforma que gestiona credenciales privilegiadas, sesiones críticas y analítica de amenazas en los entornos de sus clientes, estas vulnerabilidades deben tratarse como **prioridad alta**: un compromiso exitoso de cualquiera de estos componentes puede derivar en acceso no autorizado al Vault, escalada de privilegios en endpoints o interrupción del agente en dispositivos críticos.

A continuación se detallan las vulnerabilidades publicadas:

CA26□24 – Escalada de privilegios en EPM Windows Agent (CVSS 8.4 – High)

Impacto: Potencial escalada de privilegios no autorizada aprovechando los diálogos de Idira EPM.

Un usuario local en un endpoint podría abusar de los cuadros de diálogo configurados en el agente EPM para elevar sus privilegios más allá de lo que la política debería permitir. La falla afecta específicamente a **agentes con diálogos configurados**. No hay mitigación temporal disponible; la única solución es actualizar.

- **CVE:** N/A (no publicado en repositorios externos)
- **Productos:** EPM SaaS Windows Agent
- **Versiones afectadas:** Todas las versiones anteriores a **26.6**

CA26□25 – DoS en EPM Windows Agent por manejo incorrecto de comunicaciones internas (High)

Impacto: Potencial denegación de servicio (DoS) en el agente por manejo incorrecto de las comunicaciones internas del agente.

Un atacante o proceso malicioso en el endpoint podría provocar que el agente EPM deje de funcionar correctamente, interrumpiendo la aplicación de políticas de privilegio mínimo en el endpoint afectado. No hay mitigación temporal disponible.

- **CVE:** N/A
- **Productos:** EPM SaaS Windows Agent
- **Versiones afectadas:** Todas las versiones anteriores a **26.6**

CA26□27 – Divulgación de información en Azul Zulu / JAXP en PTA (CVSS 8.7 – High)

Impacto: Potencial divulgación de información en el componente de terceros Azul Zulu (componente JAXP) utilizado por Privileged Threat Analytics (PTA).

La vulnerabilidad, identificada como **CVE□2026□22016**, reside en la librería de terceros Azul Zulu (componente JAXP) integrada en PTA/PAM Self□Hosted. Podría permitir a un atacante obtener información sensible a través del componente de procesamiento XML. No hay mitigación temporal; se debe actualizar.

- **CVE:** CVE□2026□22016
- **Productos:** Privileged Threat Analytics (PTA), Idira PAM Self□Hosted
- **Versiones afectadas:** Todas las versiones anteriores a **15.2**

CA26□28 – Acceso no autorizado al Vault vía autenticación RADIUS (CVSS 7.7 – High)

Impacto: Potencial acceso no autorizado al Vault cuando se utiliza autenticación RADIUS.

Una vulnerabilidad en el manejo del protocolo RADIUS en el componente Vault/Infra Self□Hosted podría permitir a un atacante eludir los controles de autenticación y acceder al Vault. Tras actualizar, puede ser necesaria una **reconfiguración adicional**relacionada con mejoras de seguridad en el protocolo RADIUS; consultar el artículo FAQ dedicado en la comunidad técnica de Idira.

- **CVE:** N/A
- **Productos:** Vault / Infra Self‑Hosted
- **Versiones afectadas:** Todas las versiones anteriores a **15.0.3 (inclusive)**

CA26‑29 – Compromiso potencial del Vault vía Remote Control Client (CVSS 8.4 – High)

Impacto: Potencial compromiso del Vault a través del Remote Control Client.

El Remote Control Client es una herramienta de administración utilizada para automatizar tareas sobre el Vault y el DR Vault. La vulnerabilidad podría permitir que un actor con acceso a este cliente ejecute acciones no autorizadas sobre el Vault. No hay mitigación temporal disponible.

- **CVE:** N/A
- **Productos:** Remote Control Client
- **Versiones afectadas:** Todas las versiones anteriores a **15.0.3 (inclusive)**

Solución:

El proveedor recomienda aplicar los parches correspondientes:

Producto y versión instalada	Versión de parche recomendada	Descarga	Documentación
EPM SaaS Windows Agent – todas las versiones anteriores a 26.6 (CA26‑24, CA26‑25)	26.6	Ver documentación	Upgrade EPM Agent
PTA / PAM Self‑Hosted – versiones anteriores a 15.2 (CA26‑27)	15.2	Descargar	Upgrade PTA 15.2
PTA / PAM Self‑Hosted 15.0.x anterior a 15.0.1	15.0.1	Descargar	Upgrade PTA 15.0
PTA / PAM Self‑Hosted 14.6 (LTS) anterior a 14.6.2	14.6.2	Descargar	Upgrade PTA 14.6
PTA / PAM Self‑Hosted 14.2 (LTS) anterior a 14.2.5	14.2.5	Descargar	Upgrade PTA 14.2
PTA / PAM Self‑Hosted 14.0 (LTS) anterior a 14.0.5	14.0.5	Descargar	Upgrade PTA 14.0
Vault / Infra Self‑Hosted 15.0.x anterior a 15.0.4 (CA26‑28)	15.0.4	Descargar	Upgrade Vault 15.0
Vault / Infra Self‑Hosted 14.6.x anterior a 14.6.6	14.6.6	Descargar	Upgrade Vault 14.6
Vault / Infra Self‑Hosted 14.2.x anterior a 14.2.8	14.2.8	Descargar	Upgrade Vault 14.2

Producto y versión instalada	Versión de parche recomendada	Descarga	Documentación
Vault / Infra Self‑Hosted 14.0.x o versiones más antiguas	14.0.9	Descargar	Upgrade Vault 14.0
Remote Control Client 15.0.x anterior a 15.0.4 (CA26‑29)	15.0.4	Descargar	Upgrade Remote Control Client
Remote Control Client 14.6.x anterior a 14.6.6	14.6.6	Descargar	Upgrade Remote Control Client
Remote Control Client 14.2.x anterior a 14.2.8	14.2.8	Descargar	Upgrade Remote Control Client
Remote Control Client 14.0.x anterior a 14.0.9	14.0.9	Descargar	Upgrade Remote Control Client

Nota: para Vault/Infra (CA26‑28), tras actualizar revisar la configuración RADIUS según el artículo FAQ de la comunidad técnica de Idira.

Nota CA26‑28: si tras actualizar aparece el error ITATS108E Authentication failure, revisar el FAQ técnico CA26‑28 para la reconfiguración RADIUS requerida.

Referencias:

- Idira Security Bulletin CA26?24 – Privilege Elevation via EPM Dialogs
- Idira Security Bulletin CA26?25 – Agent DoS via Internal Communications
- Idira Security Bulletin CA26?27 – Information Disclosure in Azul Zulu/JAXP (CVE?2026?22016)
- Idira Security Bulletin CA26?28 – Unauthorized Vault Access via RADIUS
- Idira Security Bulletin CA26?29 – Vault Compromise via Remote Control Client
- Idira / CyberArk Product Security Portal