Boletín de alerta

Boletín Nro.:
Fecha de publicación: 22/04/2026
Tema: Alerta 2026-41 Multiples vulnerabilidades en ManageEngine
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- ManageEngine Password Manager Pro: versiones de la 8600 a la 13230.
- ManageEngine PAM360: versiones anteriores a la compilación 8531.
- ManageEngine Log360: versiones de la compilación 13000 a la 13013.

Descripción

Se han identificado dos vulnerabilidades críticas catalogadas como CVE-2026-3324 y CVE-2026-5785, las cuales podrían permitir a un atacante comprometer sistemas afectados dependiendo del contexto de implementación.

A continuación, se listan las vulnerabilidades y sus detalles:

- **CVE-2026-3324**: Corresponde a una vulnerabilidad de criticidad 8.2, que podría permitir la ejecución de código o manipulación de procesos internos mediante el aprovechamiento de validaciones insuficientes en componentes expuestos. La explotación exitosa podría derivar en la ejecución de comandos arbitrarios o acceso no autorizado a recursos del sistema.

- CVE-2026-5785: Se trata de una vulnerabilidad adicional con criticidad 8 que podría ser encadenada con otras debilidades para incrementar el impacto, permitiendo elevación de privilegios, acceso a información sensible o alteración del comportamiento del sistema afectado.

Ambas vulnerabilidades representan un riesgo elevado, especialmente en entornos donde los servicios vulnerables están expuestos a redes externas, existen accesos remotos sin controles robustos y no se han aplicado controles de segmentación o hardening.

El impacto potencial incluye ejecución remota de código (RCE), escalamiento de privilegios, compromiso total del sistema y movimiento lateral dentro de la red.

Solución y mitigaciones:

Se recomienda a las organizaciones implementar de manera inmediata las siguientes acciones, priorizando primero las instancias de Log360, PAM360 y Password Manager Pro expuestas a Internet o accesibles desde redes menos confiables:

- Aplicar sin demora los parches y actualizaciones de seguridad específicos para CVE-2026-3324 y CVE-2026-5785, siguiendo las guías oficiales de ManageEngine para Log360/EventLog Analyzer (https://www.manageengine.com/products/eventlog/advisory/CVE-2026-3324.html) y Password Manager Pro/PAM360 (**https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2026-5785.html**)
- Estringir estrictamente el acceso a los servicios vulnerables mediante segmentación y controles de red (ACL, VPN y enfoques de Zero Trust), limitando el acceso administrativo sólo desde redes y saltos controlados
- Habilitar e imponer autenticación fuerte (MFA) para todas las cuentas con acceso a las consolas de administración y a los módulos de reportes; revisar y reforzar las políticas de acceso remoto asegurando el uso de cuentas individuales, principios de mínimo privilegio y sesiones auditadas
- Monitorear de forma intensiva los logs de aplicación, base de datos y sistema operativo en busca de actividad anómala o indicios de explotación, especialmente consultas inusuales o cambios en cuentas privilegiadas
- Ejecutar escaneos de vulnerabilidades actualizados para identificar instancias de Log360, PAM360 y Password Manager Pro aún sin parchear, verificando la aplicación efectiva de las versiones corregidas (Log360 > 13013, PAM360 ≥ 8531, Password Manager Pro > 13230 según la guía del fabricante).

Información adicional:

- **https://www.cert.gov.py/vulnerabilidades-en-productos-manageengine/**
- **https://www.cve.org/CVERecord?id=CVE-2026-3324**
- **https://horizon3.ai/attack-research/vulnerabilities/cve-2026-3324/**
- **https://www.rapid7.com/db/vulnerabilities/zoho-manageengine-pam360-cve-2026-5785/**
- **https://asec.ahnlab.com/en/93437/**