BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-33
Fecha de publicación: 7/05/2025
Tema: Vulnerabilidades Críticas en SysAid IT
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- SysAid On-Prem <= 23.3.40

Descripción

Se han identificado y corregido tres vulnerabilidades críticas en SysAid ITSM, una plataforma ampliamente utilizada para la gestión de servicios de TI. Las fallas, reportadas bajo los identificadores CVE-2025-2775, CVE-2025-2776 y CVE-2025-2777, permiten a un atacante remoto ejecutar código arbitrario (RCE), eludir mecanismos de autenticación, escalar privilegio y acceder a información sensible del sistema.

Las vulnerabilidades, identificadas como CVE-2025-2775, CVE-2025-2776 y CVE-2025-2777, han sido descritas como inyecciones de entidad externa XML (XXE), que ocurren cuando un atacante puede interferir con éxito en el análisis de la entrada XML de una aplicación.

A continuación se detallan las vulnerabilidades:

- CVE-2025-2775 (CVSSv3 9.3)y CVE-2025-2776 (CVSSv3 9.3): Un XXE previamente autenticado dentro del punto final /mdm/checkin

- CVE-2025-2777 (CVSSv3 9.3): Un XXE previamente autenticado dentro del punto final /lshw

- CVE-2025-2778 (aún no se confirma): Las fallas XXE podrían estar asociadas con otra vulnerabilidad de inyección de comandos del sistema operativo, para lograr la ejecución remota de código (RCE). El problema de inyección de comandos se ha identificado con el identificador CVE-2025-2778.

Solución

Se recomienda actualizar SysAid IT on-premise a la última versión disponible publicada en mayo de 2025, la version 24.4.60 b16 corrige todas las vulnerabilidades mencionadas.

Las actualizaciones están disponibles en el portal oficial de SysAid:

https://documentation.sysaid.com/docs/24-40-60

Información adicional:

- https://thehackernews.com/2025/05/sysaid-patches-4-critical-flaws.html
- https://labs.watchtowr.com/sysowned-your-friendly-rce-support-ticket/
- https://www.cve.org/CVERecord?id=CVE-2025-2775
- https://www.cve.org/CVERecord?id=CVE-2025-2776
- https://www.cve.org/CVERecord?id=CVE-2025-2777
- https://www.cve.org/CVERecord?id=CVE-2025-2778

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com