Boletín de alerta

Boletín Nro.:
Fecha de publicación: 23/07/2025
Tema: Alerta 2025-64 : Explotación activa de vulnerabilidad críticas en sysaid
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- SysAid On-Prem versiones iguales o anteriores a la 23.3.40

Descripción

Se ha detectado una **explotación activa y masiva** de dos vulnerabilidades críticas en el software SysAid On-Prem, utilizado para la gestión de servicios de TI. Estas fallas de seguridad permiten a los atacantes externos tomar control total de cuentas de administrador e incluso leer archivos del sistema.

Las vulnerabilidades, identificadas como **CVE-2025-2775** y **CVE-2025-2776**, están relacionadas con un tipo de ataque conocido como **XXE (External XML Entity)**, el cual permite ejecutar acciones maliciosas sin necesidad de autenticación.

- **CVE-2025-2775:** Afecta el proceso de registro/check-in del sistema.
- **CVE-2025-2776:** Afecta el manejo de URLs del servidor.

Ambas vulnerabilidades permiten a los atacantes comprometer cuentas privilegiadas y acceder a información sensible dentro del sistema afectado.

Solución:

La empresa SysAid publicó una actualización de seguridad en la versión **24.4.60**, donde estas fallas ya fueron corregidas.

https://documentation.sysaid.com/docs/latest-version-installation-files

.

Información adicional:

- https://www.bleepingcomputer.com/news/security/cisa-warns-of-hackers-exploiting-sysaid-vulnerabilities-in-attacks/
- https://www.cisa.gov/news-events/alerts/2025/07/22/cisa-adds-four-known-exploited-vulnerabilities-catalog
- https://nvd.nist.gov/vuln/detail/cve-2025-2775
- https://nvd.nist.gov/vuln/detail/CVE-2025-2776