La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), advirtió sobre la explotación activa de dos vulnerabilidades de seguridad que afectan a la plataforma de monitoreo empresarial de código abierto Zabbix, y las agregó a su Catálogo de Vulnerabilidades Explotadas Conocidas.

Además de eso, CISA también recomienda que las agencias de la Rama Ejecutiva Civil Federal (FCEB) corrijan todos los sistemas contra las vulnerabilidades antes del 8 de marzo de 2022 para reducir su exposición a posibles ataques cibernéticos.

Rastreadas como CVE-2022-23131 con puntuación CVSS de 9.8 y CVE-2022-23134 con puntuación CVSS de 5.3, las vulnerabilidades podrían comprometer redes completas, lo que permitiría que un atacante no autenticado aumente los privilegios y obtenga acceso de administrador a Zabbix Frontend, así como realizar cambios de configuración.

A Thomas Chauchefoin, de SonarSource, se le atribuye el descubrimiento y la notificación de las dos vulnerabilidades, que afectan a las versiones de Zabbix Web Frontend hasta la 5.4.8, 5.0.18 y 4.0.36. Desde entonces, los problemas se solucionaron en las versiones 5.4.9, 5.0.9 y 4.0.37 enviadas a fines de diciembre de 2021.

Ambas vulnerabilidades son el resultado de lo que la compañía llama *«almacenamiento de sesión inseguro»*, lo que permite a los atacantes eludir la autenticación y ejecutar código arbitrario. Cabe mencionar que las fallas solo afectan las instancias donde está habilitada la autenticación de inicio de sesión único (SSO) del lenguaje de marcado de aserción de seguridad (SAML).

> *«Proporcione siempre acceso a servicios sensibles con accesos internos extendidos (por ejemplo, orquestación, monitoreo) a través de VPN o un conjunto restringido de direcciones IP, endurezca los permisos del sistema de archivos para evitar cambios no deseados, elimine los scripts de configuración, etcétera»,* dijo Chauchefoin.