La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) incluyó el miércoles una vulnerabilidad de gravedad elevada en el Protocolo de Ubicación de Servicios (SLP) en su catálogo de Vulnerabilidades Explotadas Conocidas (KEV), basándose en pruebas de una explotación activa.

Identificado como CVE-2023-29552 (calificación CVSS: 7.5), el problema se relaciona con una vulnerabilidad de denegación de servicio (DoS) que podría ser aprovechada para llevar a cabo ataques masivos de amplificación DoS.

> *«El Protocolo de Ubicación de Servicios (SLP) presenta una vulnerabilidad de denegación de servicio (DoS) que podría permitir a un atacante remoto no autenticado registrar servicios y emplear tráfico UDP falsificado para ejecutar un ataque de denegación de servicio (DoS) con un factor de amplificación significativo»,* afirmó CISA.

SLP es un protocolo que facilita que los sistemas en una red de área local (LAN) se descubran y establezcan comunicaciones entre sí.

Aunque actualmente no se conocen los detalles exactos sobre cómo se está explotando la vulnerabilidad, Bitsight previamente advirtió que esta debilidad podría ser utilizada para llevar a cabo un ataque DoS con un alto factor de amplificación.

> *«Este factor de amplificación extremadamente alto posibilita que un actor con recursos limitados tenga un impacto significativo en una red y/o servidor objetivo mediante un ataque de amplificación DoS por reflexión»,* señaló.

Dada la evidencia de ataques reales que aprovechan esta falla, se requiere que las agencias federales implementen las medidas de mitigación necesarias, incluida la desactivación del servicio SLP en sistemas que operan en redes no confiables, antes del 29 de noviembre de

2023, para proteger sus redes contra posibles amenazas.