Surgieron detalles sobre una vulnerabilidad de seguridad de alta gravedad que afecta el Protocolo de Ubicación del Servicio (SLP), que podría usarse como arma para lanzar ataques volumétricos de denegación de servicio contra objetivos.

> *«Los atacantes que explotan esta vulnerabilidad podrían aprovechar las instancias vulnerables para lanzar ataques masivos de amplificación de denegación de servicio (DoS) con un factor de hasta 2200 veces, lo que podría convertirlo en un de los ataques de amplificación más grandes jamás informados»*, dijeron los investigadores de Bitsight y Curesec, Pedro Umbelino y Marco Lux.

Se dice que la vulnerabilidad, a la que se le ha asignado el identificador CVE-2023-29552 (puntuación CVSS: 8.6), afecta a más de 2000 organizaciones globales y más de 54,000 instancias de SLP a las que se puede acceder por medio de Internet.

Esto incluye VMWare ESXi Hypervisor, impresoras Konica Minolta, routers Planex, IBM Integrated Management Module (IMM), SMC IPMI y otros 665 tipos de productos.

Los 10 principales países con la mayor cantidad de organizaciones que tienen instancias SLP vulnerables son Estados Unidos, Reino Unido, Japón, Alemania, Canadá, Francia, Italia, Brasil, Países Bajos y España.

SLP es un protocolo de descubrimiento de servicios que hace posible que las computadoras y otros dispositivos encuentren servicios en una red de área local, como impresoras, servidores de archivos y otros recursos de red.

La explotación exitosa de CVE-2023-29552 podría permitir que un atacante aproveche las instancias SLP susceptibles para lanzar un ataque de amplificación de reflexión y abrumar a un servidor de destino con tráfico falso.

Para hacerlo, todo lo que un atacante debe hacer es encontrar un servidor SLP en el puerto UDP 427 y registrar *«servicios hasta que SLP niegue más entradas»*, seguido de suplantar repetidamente una solicitud a ese servicio con la IP de la víctima como la dirección de origen.

Un ataque de este tipo puede producir un factor de amplificación de hasta 2200, dando como resultado ataques DoS a gran escala. Para mitigar la amenaza, se recomienda a los usuarios que deshabiliten SLP en los sistemas conectados directamente a Internet o, alternativamente, filtren el tráfico en el puerto UDP y TCP 427.

> *«Es igualmente importante hacer cumplir una autenticación sólida y controles de acceso, permitiendo que solo los usuarios autorizados accedan a los recursos de red correctos, con el acceso monitoreado y auditado de cerca»,* dijeron los investigadores.

La compañía de seguridad web Cloudflare, en un aviso, dijo que *«espera que la prevalencia de los ataques DDoS basados en SLP aumente de forma significativa en las siguientes semanas»* a medida que los hackers experimenten con el nuevo vector de amplificación DDoS.

Los hallazgos se producen cuando una vulnerabilidad de dos años ya parcheada en la implementación de SLP de VMware fue explotada por hackers asociados con el ransomware ESXiArgs en ataques generalizados a inicios del año.