I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Explotación de vulnerabilidad en SLP
Nivel de riesgo: Alto

II. ALERTA

El 09 de noviembre de 2023, CISA (Cybersecurity and Infrastructure Security Agency) de los Estados Unidos, reveló una falla de gravedad alta en el Protocolo de ubicación de servicios (SLP).

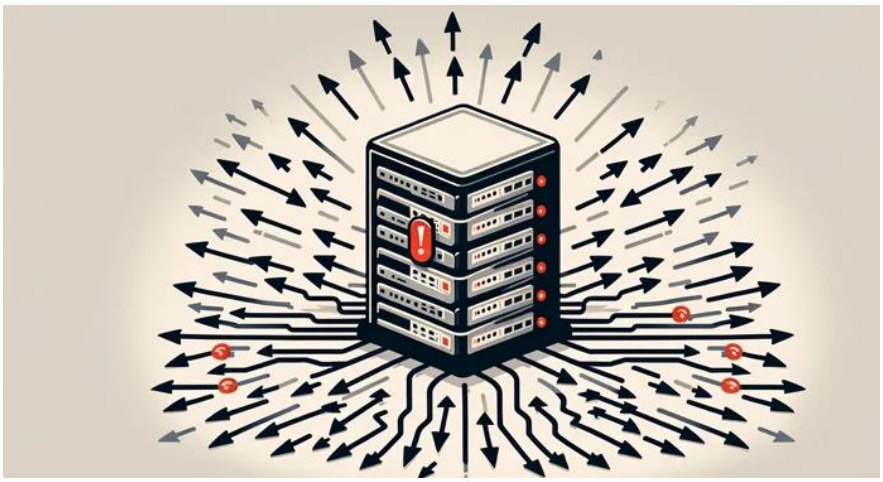

Figura No. 1.- Ilustración asociada a SLP
Fuente: https://thehackernews.com/2023/11/cisa-alerts-high-severity-slp.html

III. INTRODUCCIÓN

El Protocolo de localización de servicios (SLP) proporciona una estructura escalable para el descubrimiento y la selección de servicios de red, cuyas funciones incluyen desde servicios de hardware como, por ejemplo, los de impresoras o máquinas de fax, hasta servicios de software como los de servidores de archivos, servidores de correo electrónico, servidores web, bases de datos o cualquier otro servicio posible al que pueda accederse a través de la red.

Tradicionalmente, para utilizar un servicio determinado, una aplicación de usuario o cliente, necesita saber el nombre de host o la dirección IP del servicio. Con SLP, no es necesario para la aplicación de usuario o cliente, conocer las direcciones IP y los nombres de host individuales, la aplicación de usuario o cliente puede buscar en la red el tipo de servicio necesario y un conjunto opcional de atributos de calificación.

CISA indicó que: "El Protocolo de ubicación de servicios (SLP) contiene una vulnerabilidad de denegación de servicio (DoS) que podría permitir que un atacante remoto no autenticado registre servicios y utilice tráfico UDP falsificado para llevar a cabo un ataque de denegación de servicio (DoS) con un impacto significativo, factor de amplificación".

La vulnerabilidad SLP, fue catalogada dentro del CVE-2023-29552, con una puntuación CVSS de 7,5., publicada en abril de 2023.

IV. VECTOR DE ATAQUE:

A la fecha de elaboración de esta alerta aún se desconocen los detalles que rodean la naturaleza de la explotación de la falla, pero se advierte que la deficiencia podría explotarse para realizar ataques de denegación de servicio con un alto factor de amplificación de hasta 2200 veces.

V. IMPACTO:

El Protocolo de ubicación de servicios (SLP) permite que un atacante remoto no autenticado registre servicios arbitrarios. Esto podría permitir al atacante utilizar tráfico UDP falsificado para realizar un ataque de denegación de servicio con un factor de amplificación significativo.

VI. INDICADORES DE COMPROMISO

No aplica

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Desactivar el servicio SLP (puerto 427 UDP) en sistemas que se ejecutan en redes que no son de confianza, incluidos aquellos equipos conectados directamente a Internet.
- Actualizar los sistemas a una versión de SLP que no sea vulnerable.
- Implementar un firewall para bloquear el tráfico UDP entrante a los puertos SLP.
- Actualizar las reglas del firewall, para permitir únicamente conexiones a la infraestructura desde direcciones IP conocidas, configurar el firewall del sistema para bloquear el tráfico malicioso.

- Consultar los avisos para el CVE-2023-29552 para aplicar los parches correspondientes.
- Mantener actualizado el software del sistema operativo y las aplicaciones, pero actuar con precaución al aplicar los parches de seguridad, y utilizar los más recientes siempre que sea posible.
- Monitorear de manera proactiva las relaciones de ejecución de procesos anormales y tomar medidas preventivas para evitar actividades como la exfiltración de información.

Con estas recomendaciones de seguridad, se puede minimizar las posibilidades de ser una víctima, las recomendaciones no garantizan la seguridad, pero ayudan a reducir el riesgo.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- CVE-website. (s. f.). https://www.cve.org/CVERecord?id=CVE-2023-29552
- NVD - CVE-2023-29552. (s. f.). https://nvd.nist.gov/vuln/detail/CVE-2023-29552
- Technology, S. D. (s. f.). CISA alerts: High-Severity SLP vulnerability now under active exploitation. Seraphim Digital Technology. https://www.sdt.co.id/news/cisa-alerts-high-severity-slp-vulnerability-now-under-active-exploitation
- The Hacker News. (s. f.-a). CISA alerts: High-Severity SLP vulnerability now under active exploitation. https://thehackernews.com/2023/11/cisa-alerts-high-severity-slp.html
- The Hacker News. (s. f.-b). New SLP vulnerability could let attackers launch 2200x powerful DDoS attacks. https://thehackernews.com/2023/04/new-slp-vulnerability-could-let.html
- The Hacker News. (2023, 10 noviembre). CISA alerts: High-Severity SLP vulnerability now under active - vulnerability database | Vulners.com. Vulners Database. https://vulners.com/thn/THN:A37D839D563F178D351718B4F5CAA465
- Timalsina, R. (2023a, noviembre 10). Active exploitation of High-Severity SLP vulnerability. TuxCare. https://tuxcare.com/blog/active-exploitation-of-high-severity-slp-vulnerability/
- Timalsina, R. (2023b, noviembre 16). Active exploitation of High-Severity SLP vulnerability - Security Boulevard. Security Boulevard. https://securityboulevard.com/2023/11/active-exploitation-of-high-severity-slp-

vulnerability/?utm_source=sbwebsite&utm_medium=marquee&utm_campaign=marquee