Teléfonos IP Cisco Vulnerables A Infiltraciones En Conversaciones

Una vulnerabilidad crítica en el **firmware de los teléfonos IP de Cisco** para pequeñas empresas, permite a un atacante no autenticado espiar remotamente una conversación privada y hacer llamadas telefónicas de los dispositivos vulnerables sin necesidad de autenticarse, según ha advertido **Cisco**.

Escuchar Y Hacer Llamadas A Distancia

La vulnerabilidad (CVE-2015-0670) en realidad reside en la **configuración por defecto de determinados teléfonos IP de Cisco,** la cual se debe a la «autenticación irregular», que permite a los hackers espiar de forma remota en los dispositivos afectados por el envío de la solicitud XML especialmente diseñada.

Por otra parte, la vulnerabilidad podría ser **explotada por los hackers** para realizar **llamadas de teléfono de forma remota** desde los teléfonos vulnerables, así como para llevar a cabo otros ataques, haciendo uso de la información recogida a través de la actividad de **interceptación de audio**.

Dispositivos Afectados

Los dispositivos afectados son los modelos SPA300 y SPA500 que funcionan con el protocolo IP para pequeñas empresas de Cisco, los cuales funcionan con la **versión de firmware 7.5.5**, sin embargo, Cisco alerta de que las versiones posteriores de estos dispositivos también pueden verse afectados por la vulnerabilidad.

Es probable que algunos teléfonos se han configurado para ser accesible desde Internet, por lo que sería muy fácil para los hackers localizar los dispositivos vulnerables que se ejecutan en las versiones del software vulnerables mediante el popular **motor de búsqueda Shodan**.

> *«Para aprovechar esta vulnerabilidad, un atacante puede necesitar acceso a redes internas detrás de un firewall para enviar solicitudes XML diseñada para el dispositivo de destino», dice el aviso de Cisco. «Este requisito de acceso puede reducir la probabilidad de un ataque exitoso.»*

Cisco ha confirmado el tema, que fue descubierto y reportado por Chris Watts, investigador de Análisis Técnico en Australia, junto con otros dos defectos, una vulnerabilidad XSS (CVE-2014-3313) y una vulnerabilidad de ejecución de código local (CVE-2014 -3312).

Vulnerabilidad Sin Solución, Pero Con Algunas Recomendaciones

La compañía no ha solucionado el problema todavía y está trabajando en una **nueva versión del firmware** para solucionar el problema, aunque la compañía ofrece una serie de recomendaciones con el fin de mitigar el riesgo:

- Se recomienda a los administradores habilitar la

autenticación para la ejecución XML en el ajuste de la configuración del dispositivo afectado.

- Se recomienda a los administradores permitir el acceso a la red sólo para usuarios de confianza.
- Se recomienda a los administradores usar **estrategias de firewall** sólidas para ayudar a proteger los sistemas afectados de ataques externos.
- Los administradores también pueden utilizar las listas de control de acceso basadas en IP (ACL) para permitir que sólo los sistemas de confianza puedan acceder a los sistemas afectados.
- Los administradores se les recomienda vigilar estrechamente los dispositivos vulnerables.