Barracuda ha informado que actores cibernéticos chinos utilizaron una vulnerabilidad recién descubierta en sus dispositivos de la Puerta de Seguridad de Correo Electrónico (ESG) para instalar puertas traseras en un grupo *«reducido»* de aparatos.

Identificado como CVE-2023-7102, este problema se refiere a un incidente de ejecución de código no autorizado que se halla en una librería de código abierto llamada *Spreadsheet::ParseExcel*, la cual es empleada por el sistema Amavis en el dispositivo.

La compañía identificó a la entidad detrás de esta actividad como UNC4841, un grupo previamente relacionado con la explotación de otra vulnerabilidad en dispositivos Barracuda (puntuación CVSS: 9.8) más temprano en el año.

Para aprovechar la vulnerabilidad, se utilizó un archivo adjunto de correo electrónico con formato Excel diseñado de manera específica. Una vez infiltrado, se introdujeron nuevas versiones de programas maliciosos conocidos como SEASPY y SALTWATER, diseñados para mantener el control y ejecutar comandos.

Barracuda confirmó que ya ha puesto en marcha una actualización de seguridad, implementada automáticamente el 21 de diciembre de 2023, y asegura que los usuarios no necesitan tomar medidas adicionales.

Adicionalmente, la empresa indicó que, un día después, proporcionó una solución para los dispositivos ESG afectados por esta amenaza. No especificaron cuántos dispositivos fueron comprometidos.

Cabe destacar que la vulnerabilidad original en el módulo Perl Spreadsheet::ParseExcel (versión 0.65) aún está sin resolver y ha sido etiquetada como CVE-2023-7101, instando a los usuarios a tomar medidas correctivas.

De acuerdo con Mandiant, que ha estado monitoreando el incidente, se estima que organizaciones tanto públicas como privadas en al menos 16 naciones han experimentado consecuencias desde octubre de 2022.

Este reciente incidente demuestra una vez más la capacidad de adaptación de UNC4841, que sigue innovando en sus métodos para mantener acceso a objetivos clave a medida que las vulnerabilidades anteriores se solucionan.