ALERTA

Vulnerabilidad CVE-2023-48788 asociada a Fortinet

COLCERT AL-1909-049

TLP:CLEAR

El grupo de ransomware Medusa ha estado aprovechando una vulnerabilidad crítica en el software Fortinet FortiClient EMS para lanzar ataques sofisticados a diversas organizaciones. Estos ataques implican la exfiltración de datos y la ejecución de ransomware, lo que puede tener graves consecuencias para las víctimas. La vulnerabilidad, catalogada como CVE-2023-48788, permite a los atacantes ejecutar comandos arbitrarios en sistemas vulnerables, otorgándoles control casi total sobre los sistemas comprometidos.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

Descripción: La vulnerabilidad en FortiClient EMS permite a los atacantes ejecutar comandos arbitrarios. Esta vulnerabilidad de inyección SQL es explotada para tomar control de los sistemas afectados.

ANÁLISIS

La vulnerabilidad crítica en Fortinet FortiClient EMS, explotada por Medusa mediante inyección SQL, permite el acceso inicial no autorizado a los sistemas. Esta brecha facilita la escalada de privilegios, otorgando a los atacantes control extendido sobre la infraestructura comprometida. La vulnerabilidad es instrumental para la exfiltración de datos a través de la red Tor y el despliegue del ransomware "gaze.exe", que cifra archivos críticos.

IMPACTO PARA COLOMBIA Y LA REGIÓN

- **Pérdida de Datos:**Riesgo significativo de pérdida de datos confidenciales.
- **Interrupción Operativa:** Posibles interrupciones en las operaciones normales.
- **Daños Financieros:** Potenciales pérdidas financieras debido a pagos de rescate y recuperación.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://cybersecuritynews.com/medusa-ransomware-exploiting-fortinet-flaw/
https://www.cyberdaily.au/security/11128-exclusive-sydney-based-compass-group-confirms-medusa-ransomware-attack
https://cert.europa.eu/publications/security-advisories/2024-100/

COLCERT