Evaluación de Vulnerabilidades con CVSS v3.1

Seguridad Informatica II

Integrantes del Equipo:

Lopez Lopez Josue Emmanuel	182078
Mata Martinez Aaron Efraim	179419
Rodriguez Hernandez Edgar Omar	177888
Rodriguez Morin Estefano Alessandro	178584
Ros Padilla Ivan	177573
Salinas Carrillo Mauricio Josafat	177406

Profesor: Servando Lopez Contreras

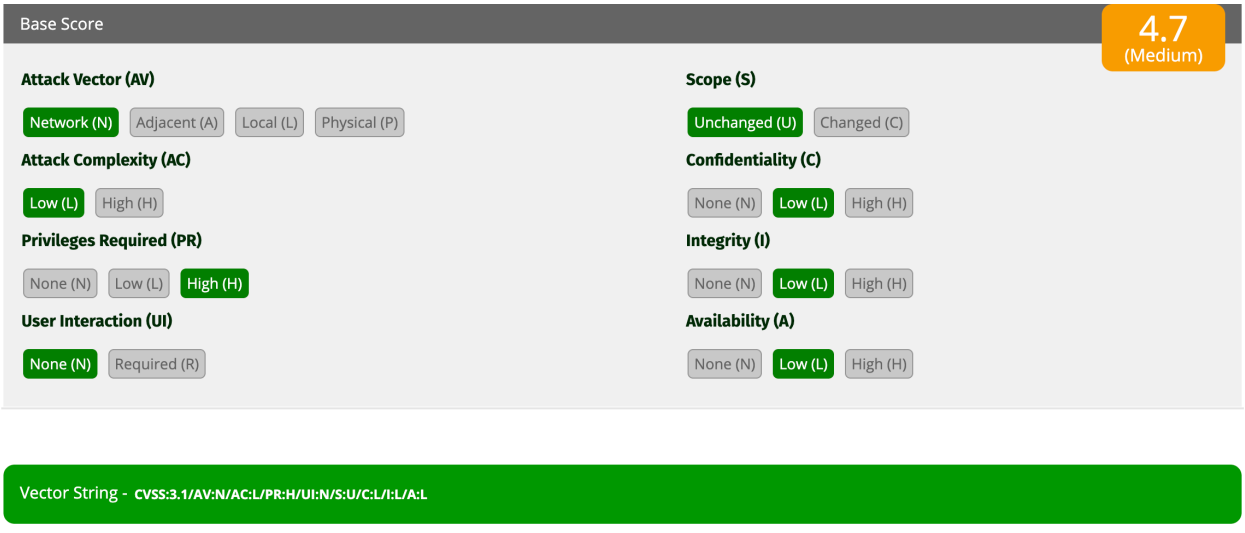
15 de mayo de 2026

Escenario:

Una organización detecta una vulnerabilidad en un sistema web interno con las siguientes características:

1. Puede explotarse a través de la red.
2. La explotación requiere baja complejidad
3. Se necesitan privilegios elevados
4. No requiere interacción del usuario
5. No cambia el alcance
6. El impacto en,
    1. Confidencialidad: Bajo
    2. Integridad: Bajo
    3. Disponibilidad: Bajo

Construcción del vector:



Interpretación técnica:

Aunque la vulnerabilidad requiere privilegios elevados, sigue siendo relevante porque puede explotarse a través de la red, con baja complejidad y sin interacción del usuario. Esto significa que, si un atacante interno, un administrador malicioso o

alguien que robó credenciales privilegiadas obtiene acceso al sistema, podría explotar la falla de manera directa. El tipo de atacante más probable sería un usuario interno con permisos altos, un administrador comprometido o un atacante externo que haya conseguido credenciales elevadas mediante phishing, robo de sesión o mala configuración. Que el impacto sea bajo en confidencialidad, integridad y disponibilidad significa que la vulnerabilidad no compromete completamente el sistema, pero sí puede causar filtración limitada de datos, modificaciones parciales o interrupciones menores del servicio. Por eso no se considera crítica, pero sí debe atenderse porque puede formar parte de una cadena de ataque más grave.

Calculo de puntuación:

Puntuación Base: 4.7

Categoría: Media (Rango de 4.0 a 6.9) se tuvo una puntuación de 4.7