

Link del video: <https://www.youtube.com/watch?v=Pk0JbYuQoIQ>

CIA TRIAD & BUSINESS IMPACT ANALYSIS



VULNERABILIDAD 1: PROFTPD MOD_COPY INFORMATION DISCLOSURE

- CIA Afectado:
Confidencialidad
- Impacto en AcmeTech:
- Permite la lectura no autorizada de archivos del sistema, incluyendo potencialmente credenciales, configuraciones o información confidencial.
- Esto puede llevar a robo de datos sensibles y dañar la confianza de los clientes.
- Mitigación:
- Deshabilitar el módulo mod_copy.
- Restringir el acceso al servicio FTP mediante listas blancas IP o VPN.



VULNERABILIDAD 2: DRUPAL CODER MODULE - REMOTE CODE EXECUTION (RCE)



- CIA Afectado: Integridad
- Impacto en AcmeTech:
- Un atacante puede ejecutar código malicioso en el servidor web, modificar contenido del sitio, insertar scripts o alterar bases de datos.
- Esto compromete la veracidad de la información que ofrece AcmeTech y pone en riesgo la reputación de la empresa.
- Mitigación:
- Actualizar Drupal y eliminar módulos innecesarios o desactualizados.
- Realizar auditorías periódicas del CMS y aplicar controles de validación de entrada.



- CIA Afectado: Disponibilidad
- Impacto en AcmeTech:
- La falta de soporte del sistema operativo lo hace altamente vulnerable a ataques conocidos, lo que puede provocar interrupciones del servicio o pérdida de control sobre el sistema.
- Un sistema fuera de línea implica pérdida de operaciones, posibles multas regulatorias y clientes insatisfechos.
- Mitigación:
- Migrar a una versión moderna y con soporte de Ubuntu (por ejemplo, 22.04 LTS).
- Implementar procesos de actualización y monitoreo de sistemas obsoletos.

VULNERABILIDAD 3: UBUNTU 14.04 END OF LIFE (SEOL)



GRACIAS