INFORME DE BUG EN API TESTING

Título del Informe: Informe de Bug Detectado en API TESTING

Autor: Elkin Favian Rios Jimenez

Cargo: Automatizador QA

Fecha de Elaboración: 21 de marzo de 2025

Empresa: DataWifi

Informe de Bug Detectado en API TESTING

Título del Bug:

Restricción en Métodos HTTP (PUT, PATCH, DELETE) en API TESTING

Fecha de Detección:

[Fecha del hallazgo]

Probado en:

- Herramienta: Postman
- URL de la API: https://api.datawifi.co/api/v2/APP-Datawifi/_table/dispositivos?api_key=b4e3a2dc334456d14a5b298e6c2f90224c2319c73b25ad7d1e47ff605a8bd428&limit=2

Descripción del Bug:

Al realizar pruebas de validación en la API TESTING usando Postman, se encontró que la API solo permite peticiones de tipo GET, rechazando cualquier intento de modificación o eliminación de datos a través de los métodos PUT, PATCH y DELETE. Además, al intentar ejecutar estas solicitudes, la API devuelve un error de autenticación (401 Unauthorized).

Pasos para Reproducir:

- Abrir Postman.

- Configurar una petición PUT, PATCH o DELETE a la URL proporcionada.

- Incluir un payload válido en la sección "Body" (para PUT y PATCH).

- Enviar la solicitud y revisar la respuesta de la API.

Resultado Esperado:

La API debería permitir modificar (PUT, PATCH) o eliminar (DELETE) registros si el usuario tiene los permisos adecuados.

Resultado Observado:

La API devuelve el siguiente error:


```
{
  "error": {
    "code": 401,
    "context": null,
    "message": "Unauthorized. User is not authenticated.",
    "status_code": 401
  }
}
```

Severidad:

Alta - Este problema impide la gestión completa de los datos a través de la API, afectando la administración de dispositivos.

Impacto:

- Los usuarios no pueden modificar ni eliminar dispositivos desde la API.
- Limitaciones en la actualización de información, lo que puede afectar la precisión de los datos almacenados.

Posibles Causas:

- Configuración de permisos en el servidor que restringe métodos PUT, PATCH y DELETE.

- Falta de endpoints habilitados para estos métodos en la API.

- Restricciones en la clave de API utilizada.

- Autenticación requerida pero no correctamente configurada en la solicitud.

Posibles Soluciones:

- Revisar Permisos del Servidor: Verificar la configuración del backend para permitir PUT, PATCH y DELETE.

- Habilitar Endpoints Faltantes: Si los métodos no están implementados, considerar su desarrollo.

- Actualizar Claves de API: Asegurar que la clave utilizada tenga los permisos adecuados.

- Autenticación Correcta: Confirmar si se requiere un token de autenticación adicional y agregarlo a las cabeceras de la solicitud.

- Consultar con el Proveedor de la API: Confirmar si estas restricciones son intencionales o un error en la configuración.

Recomendación:

Solicitar al equipo de desarrollo de la API aclarar si la restricción es intencionada. Si se requiere funcionalidad de actualización o eliminación, gestionar la habilitación de los métodos correspondientes y asegurarse de contar con la autenticación adecuada.