Path Traversal Arbitrary File

Arbitrary File Read via Path Traversal ir

BUG_Author: Chengxin Xu
Affected Version: FastBee 1.2.1
Vendor: FastBee GitHub Repository
Software: FastBee
Vulnerability Files:

- `springboot/fastbee-open-api/src/main/java/com/fastbee/data/controll`
- `springboot/fastbee-framework/src/main/java/com/fastbee/framewo`

Description

FastBee contains an arbitrary file read vulnerability in the file endpoint uses user-controlled `fileName` input to construct checks. Attackers can supply `../` path traversal sequences read arbitrary files from the server filesystem.

Path Traversal via File Download (/iot/tool/dow

The vulnerability starts from the `ToolController.downlo` parameter, strips the `/profile` prefix with a simple string r `RuoYiConfig.getProfile()`, and directly reads the res

Entry Point (ToolController.java:350-367):

Code block

```
@GetMapping("/download")
public void download(String fileName, HttpSe
    try {
//              if (!FileUtils.checkAllowDownl
```