

New issue

[Jump to bottom](#)

# Arbitrary file reading vulnerability exists in the ve-plus3.6.0

## #85

🔓 Open lanfei-4 opened this issue on Apr 3 · 0 comments

lanfei-4 commented on Apr 3

Vulnerable code:

```
`@RequestMapping(value = "/download")
public void fileDownload(String filePath,String fileName, HttpServletResponse resp) throws Exception {
    String realFilePath = jnConfig.getUploadPath() + filePath;
    InputStream in = new FileInputStream(realFilePath);
    //设置响应头，对文件进行url编码
    fileName = URLEncoder.encode(fileName, "UTF-8");
    resp.setHeader("Content-Disposition", "attachment;filename=" + fileName);

    resp.setContentLength(in.available());

    OutputStream out = resp.getOutputStream();
    byte[] b = new byte[1024];
    int len = 0;
    while ((len = in.read(b)) != -1) {
        out.write(b, 0, len);
    }
    out.flush();
    out.close();
    in.close();
}`
```

4/5000

Burp Suite Professional v2.0.03beta - Temporary Project - licensed to By Jas502n

Done 1,194 bytes | 9 millis

No one assigned

None yet

None yet

No milestone

No branches or pull requests

