

README.md

# CVE-2018-1335

Apache Tika-server with version below 1.18 allow code injection via carefully crafted headers.

## Exploit Details

The path `/meta` allows PUT request and the header information can be obtained from the source code of the tika server. The `processHeaderConfig` definition is run on the `ocrConfig` object when the prefix of the header is `X_TIKA_OCR`. The `TesseractPath` is used in construction of an array of strings that will be used for construction of command for `ProcessBuilder`. There is no sanitation on these strings.

When passing the request, we need to send it as an image. The Tika server will check the magic bits for the given data. But when the content type is defined, it will not check them and hence by adding that header, it is possible to inject any data.

## Example

```
python exploit.py host port notepad.exe
```

The above one will start a notepad on the remote server.

