

https://www.knownsec.com?from=seebug_logo

(/)

泛微OA SQL注入漏洞



☆ Follow 0

SSV ID:SSV-98091 (/help/vul#ssv)

Find Time:Unknown

Submit Time:2019-10-18

Level:

Category:SQL 注入 (/category/sql-injection)

Component:e-cology (/appdir/e-cology)

Author:Unknown

Submitter:Knownsec (/accounts/profile/admin)

CVE-ID : Add

CNNVD-ID : Add

CNVD-ID : Add

ZoomEye Dork : Add

Source

[https://mp.weixin.qq.com/s?](https://mp.weixin.qq.com/s?__biz=MzI4NjE2NjgxMQ==&mid=2650240248&idx=2&sn=2dbcca413b7e774bd19d33b2b37f985e&uin=MjI1MzE0ODA3NQ%3D%3D&devicetype=Windows+10&version=62070141&lang=zh_CN)[__biz=MzI4NjE2NjgxMQ==&mid=2650240248&idx=2&sn=2dbcca413b7e774bd19d33b2b37f985e&uin=MjI1MzE0ODA3NQ%3D%3D&devicetype=Windows+10&version=62070141&lang=zh_CN](https://mp.weixin.qq.com/s?__biz=MzI4NjE2NjgxMQ==&mid=2650240248&idx=2&sn=2dbcca413b7e774bd19d33b2b37f985e&uin=MjI1MzE0ODA3NQ%3D%3D&devicetype=Windows+10&version=62070141&lang=zh_CN)[https://mp.weixin.qq.com/s?](https://mp.weixin.qq.com/s?__biz=MzI4NjE2NjgxMQ==&mid=2650240248&idx=2&sn=2dbcca413b7e774bd19d33b2b37f985e&uin=MjI1MzE0ODA3NQ%3D%3D&devicetype=Windows+10&version=62070141&lang=zh_CN)[__biz=MzI4NjE2NjgxMQ==&mid=2650240248&idx=2&sn=2dbcca413b7e774bd19d33b2b37f985e&uin=MjI1MzE0ODA3NQ%3D%3D&devicetype=Windows+10&version=62070141&lang=zh_CN\)](https://mp.weixin.qq.com/s?__biz=MzI4NjE2NjgxMQ==&mid=2650240248&idx=2&sn=2dbcca413b7e774bd19d33b2b37f985e&uin=MjI1MzE0ODA3NQ%3D%3D&devicetype=Windows+10&version=62070141&lang=zh_CN)

Detail

Contributor (/accounts/profile/None) Got 0KB

泛微OA介绍

泛微成立于2001年，总部设立于上海，专注于协同管理OA软件领域，并致力于以协同OA为核心帮助企业构建全新的移动办公平台。

漏洞描述

该漏洞属于泛微OA的通用型漏洞，攻击者可以通过精心构造的语句进行注入攻击，成功利用漏洞的攻击者可以获取服务器中的数据。

漏洞复现

深信服安全人员通过尝试，复现此漏洞，验证效果如下图：

影响范围

目前据统计，在全球范围内对互联网开放泛微OA的资产数量多达6000多台，其中大多数均为国内的设备。

修复建议

官方已经针对此漏洞发布修复补丁，请联系厂商获取漏洞最新状态与补丁更新：

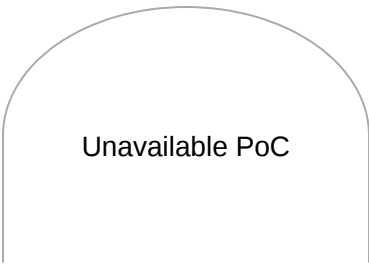
下载链接：

<https://www.weaver.com.cn/cs/securityDownload.asp>

(<https://www.weaver.com.cn/cs/securityDownload.asp>)

have 0 exchange

PoC



Unavailable PoC



Reference Linking

Solutions

Temp Solutions

Unavailable Temp Solutions

Official Solution

Unavailable Official solution

Defense Solutions

Unavailable Defense Solutions

Improve Solutions

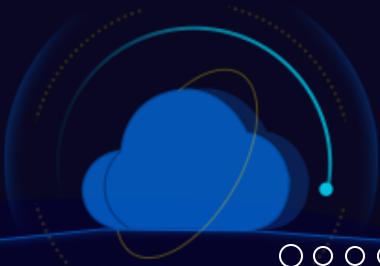


知道创宇云安全

Web云防御行业领导者

恶意流量清洗 安全CDN加速 全方位防黑服务

免费接入



(<https://www.vulnab.com/>)

Timeline

发现/披露了漏洞



(/accounts/profile/admin) Knownsec (/accounts/profile/admin) +

2019-10-18 提交了漏洞



(/accounts/profile/admin) Knownsec (/accounts/profile/admin) +

2019-10-18 提交补充了漏洞详情

Related Vuls

[E-cology10远程代码执行漏洞 \(/vuldb/ssvid-99871\)](#)[ecology filedownload 目录穿越漏洞 \(/vuldb/ssvid-99409\)](#)[泛微OA validate.jsp SQL注入漏洞 \(/vuldb/ssvid-99408\)](#)[泛微 OA SyncUserInfo SQL 注入漏洞 \(/vuldb/ssvid-99405\)](#)[泛微ResourceServlet任意文件下载漏洞 \(/vuldb/ssvid-99404\)](#)[泛微E-cology OA数据库配置信息泄露漏洞 \(/vuldb/ssvid-98093\)](#)[泛微OA SQL注入漏洞 \(/vuldb/ssvid-98091\)](#)[泛微e-cology OA系统存在SQL注入漏洞 \(/vuldb/ssvid-98083\)](#)[泛微 E-cology /js/jquery/plugins/jqueryFileTree/connectors/jqueryFileTree.jsp 参数dir目录遍历漏洞 \(/vuldb/ssvid-92362\)](#)[泛微 E-cology weaver.file.SignatureDownLoad 注入漏洞 \(/vuldb/ssvid-92341\)](#)

☆ Follow 0

Popularity 13441



1

Need to bind phone before comment. Bind Now (https://sso.telnet404.com/accounts/bind_phone/)

Submit Comment

☐ anonymous reply

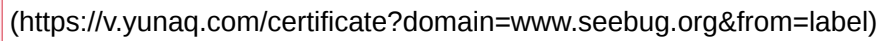
Unavailable Comments

※Any content provided by this site, only to learn the code and services, not for illegal purposes

Vulnerabilities	More	Help
Vulnerability List (/vuldb/vulnerabilities)	Reward List (/vuldb/reward/poc)	About (/help/about)
Component Categories (/appdir/)	Rank (/hackers)	Relevant Instructions (/help/user_level)
Vulnerability Category (/category/)		Vulnerability Definition (/help/vul)
		Reward Plan (/help/reward)
Contact		Public links
☎ 010-57076191		Knownsec
✉ s1@seebug.org		(https://www.knownsec.com/#/)
📍 15th Floor, Unit A, Tower 3, Wangjing SOHO, Fu'an West Road, Chaoyang District, Beijing 100102, P.R.China		yunaq (https://www.yunaq.com/cyd/?from=cj_cyd_sbug)
		创宇蜜罐-诱捕溯源
		(https://mg.yunaq.com/#/?from=seebuglink)

hackernews (<http://hackernews.cc/>)


```
idkey(http://192.168.1.170:8080/generate11ca07c70ad45fdd677e9b1e0c827845e331)
```



(/)

(<https://www.yunaq.com/?from=sbg0702>)



6/6