泛微家的产品,市面上有很多。 想搞,首先要知道哪个是哪个。 给一张历史漏洞的大概截图这里可以看一下。

泛微(Weaver-Ecology-OA)

• [2021.01.07] - 泛微OA E-cology RCE(CNVD-2019-32204) - 影响版本7.0/8.0/8.1/9.0

• [2021.01.07] - 泛微OA WorkflowCenterTreeData接口注入(限oracle数据库)

• [2021.01.07] - 泛微ecology OA数据库配置信息泄露

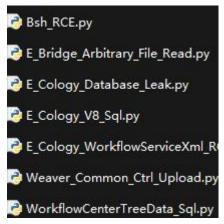
• [2021.01.07] - 泛微OA云桥任意文件读取 - 影响2018-2019 多个版本

• [2021.01.07] - 泛微 e-cology OA 前台SQL注入漏洞

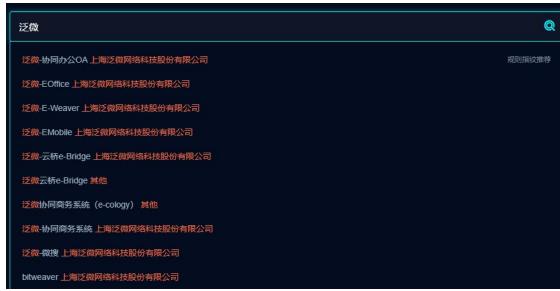
• [2021.01.07] - 泛微OA系统 com.eweaver.base.security.servlet.LoginAction 参数keywordid SQL注入漏洞

• [2021.01.07] - 泛微 OA sysinterface/codeEdit.jsp 页面任意文件上传

• [2021.01.07] - 泛微ecology OA数据库配置信息泄露



上面的漏洞列表和 poc 都是参考 github 上的资料。 再放一张 fofa 截图:



我们可以看到,上面有 ecology,有泛微 oa,有 oa 云桥,有 e-bridge,这么多相似的名字,是不是看起来有点头晕呢?那么到底什么是什么呢? 下面我们就来区分一下

泛微 Ecology

fofa 关键字: app="泛微-协同办公 OA"

这个搜到的是泛微的 ecology,ecology 是泛微针对大型企业研发的 oa。 hvv 的时候遇到的非常多,请重点关注。

Ecology 同时也是泛微家的旗舰产品,现在已经更新到 9 了,长这个样子。

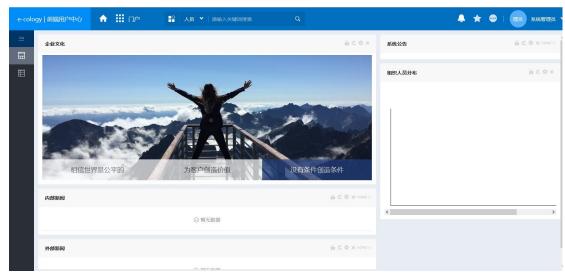


指纹:

就是这个 url,wui/index.html

localhost/wui/index.html?time=1651403158753#/?_key=f0rd63

记住这个 wui 就行,很好记 登进去之后,原始后台长这个样子



比较的空旷,左上角会写明是 ecology。

泛微 Eoffice

Fofa 关键字:

app="泛微-EOffice"

Eoffice 是泛微针对中小企业研发的 oa,功能没那么复杂,hvv 目标也有,但是少。前台长这个样子



如果没改过 ui, 就是这个样子



上面是会有 eoffice 的水印的。

指纹:

/general/login/index.php

记住这个 general

泛微 e-bridge

Fofa 关键字: app="泛微-云桥 e-Bridge" e-bridge 是一个集成平台,作用看这段介绍:

"泛微云桥e-bridge平台"是在原有微信集成平台的基础上,经过二次更新后的一款独立外部对接平台,其主要作用是实现泛微OA平台与微信企业号、阿里<u>钉钉</u>产品的信息对接能力。系统对接后,企业内部的OA信息通过微信企业号、阿里钉钉这一终端入口释放出来。

//https://www.weaver.com.cn/subpage/aboutus/news/news-detail-9345.html 目标也有,但是相对较少。

长这个样子:



这个就不用指纹了,看一眼就知道了。

泛微 e-mobile

Fofa 关键字: app="泛微-EMobile"

Emobile 是泛微家的移动端 oa,大概可以这么理解

长这个样子:



指纹是这个 icon



老版本的 icon 是这个



长这个样子



Button 部分会有自己的识别标。 有遇到,但是不多。

以上泛微家主流的几款产品,ecology,eoffice,ebridge,emobile,就介绍完毕了,在 攻防的时候,务必要一眼认出来,这是基本要求。

打攻防其实就跟做数学考试一样,在卷子上看到了熟悉的题,直接就写答案,不熟悉, 就得临时想办法,时间上就耽误了。

所以提前熟悉主流产品是很关键的,相当于熟悉题型。

然后上面这几个模块,重要程度 ecology>eoffice=ebridge>emobile。

按我讲,除了 ecology,泛微家其他组件我都懒得挖,因为市面上的 oa 不只泛微一家,还有通达,用友,蓝凌,万户,致远等等。

那么面对不那么主流的系统,出于时间成本和回报考虑,熟悉一下历史的洞就行了,到时候能打就打,不能打就拜拜,更多的时间,可以去挖别家的主流系统,因为覆盖面更广。

泛微的产品就介绍到这里,历史漏洞总结会放在另一篇来写,避免文章过于臃肿。 done