微 OA365 办公系统存在 str2 漏洞

微 OA365 **存在 str2045 和 str2046 漏洞**

所属厂商：广州市天翎网络科技有限公司（http://www.teemlink.com/）
所属产品：微 OA365 （http://www.weioa365.com/）
影响版本： weioa365 24998 以及以前版本（或者升级日期在 2016-11-24 以前的版本）

漏洞详情：

如参数: loginWithCiphertext.action

我们采用 fofa 搜索试试：
https://fofa.so/result?q=loginWithCiphertext.action&qbase64=bG9naW5XaXRoQ2lwaGVydGV4dC5hY3Rpb24%3D

取出几个 url(都存在 045 与 046 漏洞的，测试过程发现有的站点部署有 waf 需要切换 ip 测试)：

http://59.41.223.238:8080/Z02G1IEY/portal/login/loginWithCiphertext.action

http://120.76.130.3:8080/Z01R1IH8/portal/login/loginWithCiphertext.action

http://118.190.50.111/Z01R3B/portal/login/loginWithCiphertext.action;jsessionid=836B52A9862

F07F0E9A0933A06435F7D 安定区人力资源综合管理平台

http://218.59.190.74:8080/portal/login/loginWithCiphertext.action;jsessionid=E64A2B8C1E67F43CFBB15AFA510B3945 华东电缆

测试华东电缆：

http://218.59.190.74:8080/portal/login/loginWithCiphertext.action;jsessionid=E64A2B8C1E67F43CFBB15AFA510B3945

过程如下：

查看当前权限：

查看进程：

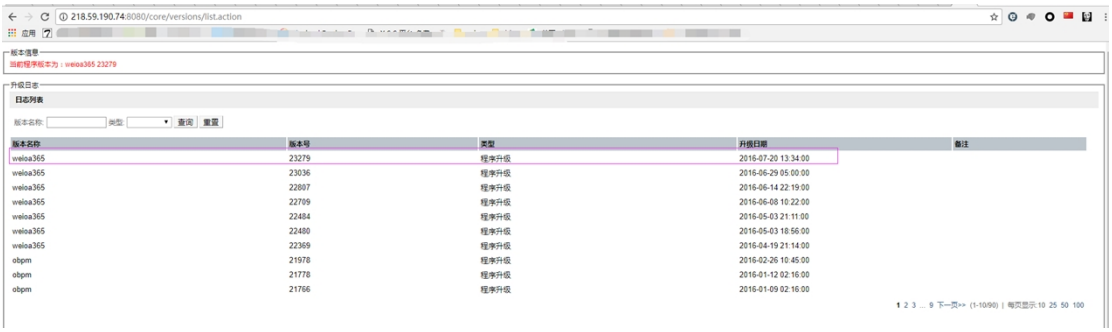
查看 arp 情况:

独立 IP:

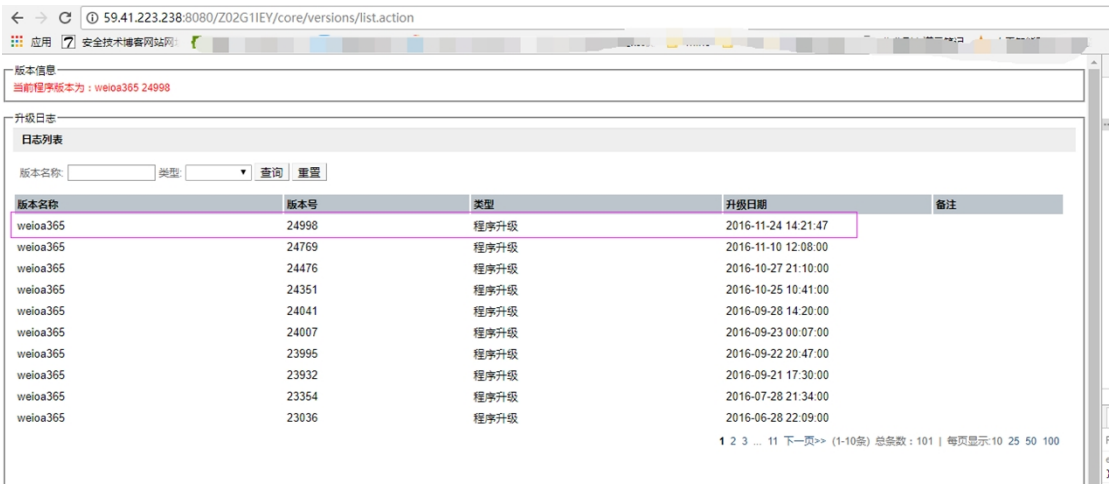
看看一些版本：

版本：

http://218.59.190.74:8080/core/versions/list.action 华东电缆 版本 weioa365 23279



http://59.41.223.238:8080/Z02G1IEY/core/versions/list.action 佳都新太科技股份有限公司 版本 weioa365 24998 升级时间 2016-11-24 14:21:47



发现影响版本在
weioa365 24998 2016-11-24 14:21:47 以及以前的。