2023 攻防演习每日情报汇总

漏洞盒子

2023-8-10

第二天看似风平浪静,实则暗流涌动。小道消息表示已经有单位出局了,但是最后证实其实是开玩笑活跃气氛,可见大家对这次演习心情既兴奋又紧张。我们看看今天又有那些资讯吧!

1、漏洞情报简讯

今日斗象漏洞情报中心通过情报星球社区捕获大量的 Oday 漏洞,以下是今日捕获的 Oday 漏洞及 nday 漏洞列表。

1.1 漏洞简讯

- 某友移动某系统任意文件上传漏洞:漏洞漏等级严重,确认 nday漏洞,POC公开。披露时间:2023/7/11
- **飞某联 OA 文件读取漏洞:**漏洞漏等级高危,确认 0day漏洞,POC 小范围流传;影响至最新版,漏洞披露时间:2023/8/10
- 某神 SecGate 3600 防火墙任意文件上传漏洞:漏洞漏等级严重, 0day 漏洞, POC 小范围流传;影响至最新版,漏洞披露时间: 2023/8/10
- 某华 DSS 平安城市 远程代码执行漏洞:漏洞漏等级严重,可能为 0day 漏

洞, POC 小范围流传; 影响版本未知, 漏洞披露时间: 2023/8/10

- 某软反序列化漏洞:漏洞漏等级严重,可能为 0day漏洞;影响版本未知, 听说有厂商已经由于该漏洞被打进去,漏洞披露时间:2023/8/10
- 某麒麟堡垒机系统 SQL 注入漏洞:漏洞漏等级高危,可能为 0day 漏洞; 影响版本未知,漏洞披露时间: 2023/8/10
- 某盟 SAS 堡垒机 Exec 远程命令执行漏洞:漏洞漏等级严重,可能为 Oday漏洞;影响版本未知,漏洞披露时间: 2023/8/10
- 某捷 NBR 路由器任意文件上传漏洞:漏洞漏等级严重,可能为 Oday 漏洞; 影响版本未知,漏洞披露时间: 2023/8/10
- 某华三虚拟授权管理系统系统命令执行漏洞:漏洞漏等级严重,可能为 Oday漏洞;影响版本未知,漏洞披露时间: 2023/8/10
- **某华三综合日志审计平台系统命令执行漏洞:**漏洞漏等级严重,可能为 0day 漏洞;影响版本未知,漏洞披露时间: 2023/8/10
- 某石网科 EDR 系统 PHP 模块命令执行漏洞:漏洞漏等级严重,可能为 0day漏洞;影响版本未知,漏洞披露时间: 2023/8/10

1.2 红队投毒案例精选

● 红队钓鱼邮件样本

斗象情报中心侦测到红队钓鱼邮件样本,样本 md5: 951cfede765818168ee b5b416d58901e704b2909300ab268c495ce6cc3a591fe。

经大圣云沙箱检测此样本为高危文件



文案内容如下

本人实名举报贵公司员工多次婚内出轨及对我进行家暴行为。 我还是太软弱了,即使在他多次家暴我,我还是没有勇气将他的揭发, 但是他的所作所为令我再也无法忍受,我彻底崩溃了,再也无法相信自己这么多年过着的 生活是怎样的。

T A

在此! 我举报此人工作作风及个人品德问题!

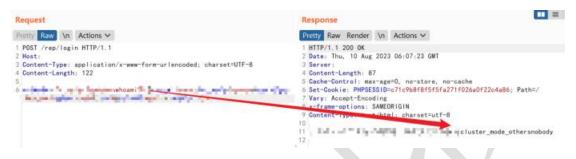
其外链地址为: service-055xw48d-1309846010.sh.apigw.tencentcs.com 请及时封禁此域名。

2、 漏洞验证及复现

2.1 某服应用交付报表系统 远程命令执行漏洞

由于系统未对用户输入进行过滤,未授权攻击者可以直接执行命令。

漏洞复现截图:



修复建议:

请使用该产品的用户尽快更新最新版本。

2.2 某神 SecGate3600 防火墙存在任意文件上传漏洞

系统未对用户输入内容进行过滤,导致攻击者可以上传恶意 Webshell 文件。

漏洞复现截图:

```
400 Washing while thick of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     has considered a province of the constraint of t
    Angle having the different
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  material residence, where programmed their
    And providing the second section in the sec
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     One old and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  atagga i watagsa.
Nasathan i Inginahanka pamomis
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              trades made in a finally compared to design the compared to design the compared to the contract of the contrac
                                months and the development in White Advance to the School of

    a semble or manufactory by training on highly

             printedlight day for the standard fold and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Olar broading and say sacropology unlimber-
    mage, magester a magester make the train of the analysis and the second control of the s
      13
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           15
        <?php system("id");unlink(__FILE__);?>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         [name] -> vulntest.php
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           18
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              --[type] -> text/plain

    Jan Horbston Verjassferetgrill

                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             19
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           [tmp_name] -> /tmp/phpzhMbhN
        System Drymitteen Hertilder, meer Societ, peer 🧟
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             28
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         --[error] => 0
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           21
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            --[size]-=>-40
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             22
                                             - mintless of recommendate to the Lineage.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           23
      prove against in the way, was finer [1]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             25
        PATHINGS SELECTION OF SELECTION
                 --- Breit of creations sorts to conside yo
```

修复建议:

请使用该产品的用户尽快收缩资产,不要将其暴露在公网中。

2.3 某友移动某系统 uploadApk.do 任意文件上传漏洞

系统未对用户输入内容进行过滤,导致攻击者可以上传恶意 Webshell 文件。

漏洞复现截图:

```
MQT Square in incompany to the large sport (90) as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             HTTP/1.1-200-0K
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Server: Apache-Coyote/1.1
To that I got had to perform one or in the state of the complete of all the state of the complete of all the state of the complete of all the complete of the 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               Content-Type: application/json; charset=utf-8
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Date: Thu, 10-Aug-2023-07:18:09-GMT
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Connection: close
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Content-Length: 19
 Assertion of the first part of the following production of the production of the profession of the following production of the production of the following production of the p
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             --- "status": 2
 College Consultate |
                                 ine It in the server of the High of S
 Europe Deposition (Consideration), Specialists (Character Special
 Charles Paper Appellant declarates
 hello
 or a deposit analysis of the talgrounding
    GET , SAME SEED TO SEE THE HTTP/1.1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        HTTP/1.1-200-OK
    Host:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Server: Apache-Coyote/1.1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Set-Cookie: JSESSIONID=066
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Path=/; HttpOnly
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Content-Type: text/html; c
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Date: Thu, 10 Aug 2023 07:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Content-Length: 5
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        hello
```

修复建议:

请使用该产品的用户尽快收缩资产,不要将其暴露在公网中;或使用 WAF 设备 对请求进行过滤。

2.4 飞某联 OA 文件读取漏洞

系统没有对用户输入进行过滤,导致攻击者可以读取服务器中的任意文件。

漏洞复现截图:

修复建议:

目前厂商暂未发布修复措施解决此安全问题,建议使用此软件的用户随时关注厂



3、 情报星球社区精选

我们看看今天情报星球社区都在热议什么:

1. 某 Q 疑似存在远程代码执行

https://planet.vulbox.com/detail/MTM4MDA=

2. 某盟 SAS 安全审计系统疑似曝出任意文件读取漏洞

https://planet.vulbox.com/detail/MTM3ODY=

3. 某 SecGate3600 防火墙存在任意文件上传漏洞

https://planet.vulbox.com/detail/MTM4NDI=

本漏洞斗象情报中心已经复现验证, 具体详情可参考以下链接:

https://vip.tophant.com/detail/1689575442991943680

4. 某友移动某系统 uploadApk.do 任意文件上传漏洞

https://planet.vulbox.com/detail/MTM4Mjg=

本漏洞斗象情报中心已经复现验证,具体详情可参考以下链接:

https://vip.tophant.com/detail/1689574635768778752

- 5. 疑似 Coremail 邮件系统未授权访问获取管理员账密,已经辟谣该消息为假https://planet.vulbox.com/detail/MTM4Njc=
- 6. 小道消息疑似态势感知出现漏洞导致出局

https://planet.vulbox.com/detail/MTM4MTU=

『情报星球』是漏洞盒子平台旗下安全情报交流与分享社区。近期社区推出攻防 演练情报奖励计划,欢迎参与: https://activity.vulbox.com/awardPlan 更多情报讨论与分享请访问『漏洞盒子-情报星球』:

https://planet.vulbox.com



扫码关注情报星球

手机看情报, 把安全装进口袋



4、 疑似红队攻击 IP 汇总

斗象情报中心在攻防第二日捕获大量疑似红队攻击 IP 地址,蓝队可根据地址针对性设置防御策略:

时间	IP 地址	归属地
8/10/2023	183.94.172.105	湖北武汉市
8/10/2023	103.231.248.56	新加坡
8/10/2023	45.95.146.70	欧盟
8/10/2023	182.96.70.74	江西南昌市
8/10/2023	111.48.159.134	湖北
8/10/2023	122.239.182.125	浙江温州市
8/10/2023	111.224.11.243	河北石家庄市
8/10/2023	111.72.192.187	江西鹰潭市
8/10/2023	106.113.15.68	河北石家庄市
8/10/2023	111.183.66.54	湖北武汉市
8/10/2023	175.154.213.161	四川德阳市
8/10/2023	220.170.69.208	湖南衡阳市
8/10/2023	35.177.51.253	美国华盛顿州西雅图市亚马逊
		(Amazon)公司数据中心
8/10/2023	171.113.48.195	湖北武汉市
8/10/2023	218.71.6.106	浙江温州市
8/10/2023	27.17.62.202	湖北武汉市

8/10/2023	117.136.23.203	湖北
8/10/2023	114.102.44.175	安徽马鞍山市
8/10/2023	218.71.10.221	浙江温州市

更多疑似红队攻击 IP 请参考情报星球:

https://planet.vulbox.com/detail/MTM4NzQ=



附录 hw 漏洞情报清单(该清单漏洞还未全部确认真实性):

爆发日期	漏洞名称
2023/8/9	某服应用交付系统命令执行
2023/8/9	协同办公文档(DzzOfffice)未授权访问
2023/8/9	某微 OA 前台代码执行漏洞
2023/8/9	某微 oa 进后台漏洞
2023/8/9	Ucl*ud 的未授权获取任意用户 cookie
2023/8/9	某书客户端 RCE 漏洞
2023/8/9	某微 Eoffice V10 前台 RCE
2023/8/9	某客推商城任意文件上传
2023/8/9	某玥堡垒机 Oday
2023/8/9	某御运维审计与风险控制系统堡垒机任意用户注册
2023/8/9	XX 协同管理系统存在 SQL 注入
2023/8/9	某微 emobile 注入漏洞
2023/8/9	海**视综合安防前台文件上传漏洞
2023/8/9	某凌 OA 前台代码执行漏洞
2023/8/9	某远 M3Server-xxxx 反序列化漏洞
2023/8/9	某远 A8 V8 SP1 SP2 文件上传漏洞
2023/8/9	某元 EOS 前台代码执行漏洞
2023/8/9	某微 E-cology 后台文件上传漏洞
2023/8/9	某微 E-Mobile 任意用户登录

2023/8/9	某微 E-Office10 信息泄露后台+后台文件上传漏洞
2023/8/9	某锁电子签章系统 RCE
2023/8/9	某通电子文档平台文件上传漏洞
2023/8/9	Idocview 命令执行漏洞
2023/8/9	jeesite 代码执行漏洞
2023/8/9	LiveBOS 文件上传漏洞
2023/8/9	某友 nc-cloud-任意文件写入
2023/8/9	某安信 VPN PWN
2023/8/9	xx IOA PWN
2023/8/9	xxx 准入 PWN
2023/8/9	eoffice9 前台文件包含
2023/8/9	某微 E-Cology
	ifNewsCheckOutByCurrentUser SQL 注入漏洞
2023/8/9	fastjson 版本<2.0.27 存在高危反序列化漏洞
2023/8/9	W*S 0day
2023/8/9	某软 channel 序列化
8/9/2023	宏某 SQL 注入漏洞
8/9/2023	某微 E-Office9 文件包含漏洞
8/9/2023	某山 WPS 存在高危 Oday 漏洞
8/9/2023	某服应用交付报表系统 远程命令执行漏洞
8/9/2023	某帆 OA SQL 注入漏洞(1day)

8/9/2023 某软反序列化漏洞绕过漏洞 8/9/2023 某华智慧园区综合管理平台 SQL 注入漏洞 8/9/2023 宏某 eHR OfficeServer.jsp 任意文件上传漏洞 8/9/2023 某达 OA SQL 注入漏洞(CVE-2023-4165) 8/9/2023 某被 e-Office ajax.php 任意文件上传漏洞 (CVE-2023-2523) 8/9/2023 某微 e-Office9 文件上传漏洞 (CVE-2023-2648) 8/9/2023 Exchange Server 远程代码执行漏洞 (CVE-2023-38182) 8/9/2023 某速 OA wpsAssistServlet 任意文件上传漏洞 果捷 RG-BCR860 后台命令注入 (CVE-2023-3450) 8/9/2023 某迈特 在特定场景下设置 Token 回调地址漏洞 果恒明御运维审计与风险控制系统 service 任意 用户添加漏洞 8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644) 8/9/2023 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898) 8/9/2023 某联达 OA SQL 注入漏洞		
### Style="color: blue;"> Style="blue;"> Style="bl	8/9/2023	某软反序列化漏洞绕过漏洞
	8/9/2023	某华智慧园区综合管理平台 SQL 注入漏洞
8/9/2023 某达 OA SQL 注入漏洞(CVE-2023-4166) 8/9/2023 某微 e-Office ajax.php 任意文件上传漏洞 (CVE-2023-2523) 8/9/2023 某微 e-Office9 文件上传漏洞 (CVE-2023-2648) 8/9/2023 Exchange Server 远程代码执行漏洞 (CVE-2023-38182) 8/9/2023 某远 OA wpsAssistServlet 任意文件上传漏洞 8/9/2023 某速 RG-BCR860 后台命令注入 (CVE-2023-3450) 8/9/2023 某迈特 在特定场景下设置 Token 回调地址漏洞 8/9/2023 某恒明御运维审计与风险控制系统 service 任意用户添加漏洞 (CVE-2023-34644) 8/9/2023 某值明御安全网关 命令执行漏洞 (CNVD-2023-03898)	8/9/2023	宏某 eHR OfficeServer.jsp 任意文件上传漏洞
8/9/2023 某微 e-Office ajax.php 任意文件上传漏洞 (CVE-2023-2523) 8/9/2023 某微 e-Office9 文件上传漏洞 (CVE-2023-2648) 8/9/2023 Exchange Server 远程代码执行漏洞 (CVE-2023-38182) 8/9/2023 某远 OA wpsAssistServlet 任意文件上传漏洞 (CVE-2023-3450) 8/9/2023 某迈特 在特定场景下设置 Token 回调地址漏洞 某恒明御运维审计与风险控制系统 service 任意 用户添加漏洞 (CVE-2023-34644) 8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644) 8/9/2023 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898)	8/9/2023	某达 OA SQL 注入漏洞(CVE-2023-4165)
(CVE-2023-2523)	8/9/2023	某达 OA SQL 注入漏洞(CVE-2023-4166)
8/9/2023 某微 e-Office9 文件上传漏洞 (CVE-2023-2648) 8/9/2023 Exchange Server 远程代码执行漏洞 (CVE-2023-38182) 8/9/2023 某远 OA wpsAssistServlet 任意文件上传漏洞 8/9/2023 某捷 RG-BCR860 后台命令注入 (CVE-2023-3450) 8/9/2023 某迈特 在特定场景下设置 Token 回调地址漏洞 8/9/2023 某恒明御运维审计与风险控制系统 service 任意 用户添加漏洞 8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644) 8/9/2023 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898)	8/9/2023	某微 e-Office ajax.php 任意文件上传漏洞
(CVE-2023-2648) Exchange Server 远程代码执行漏洞 (CVE-2023-38182) 8/9/2023 某远 OA wpsAssistServlet 任意文件上传漏洞 8/9/2023 某捷 RG-BCR860 后台命令注入 (CVE-2023-3450) 8/9/2023 某迈特 在特定场景下设置 Token 回调地址漏洞 8/9/2023 某恒明御运维审计与风险控制系统 service 任意 用户添加漏洞 8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644) 8/9/2023 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898)		(CVE-2023-2523)
Exchange Server 远程代码执行漏洞 (CVE-2023-38182) 8/9/2023	8/9/2023	某微 e-Office9 文件上传漏洞
(CVE-2023-38182)		(CVE-2023-2648)
8/9/2023 某远 OA wpsAssistServlet 任意文件上传漏洞 8/9/2023 某捷 RG-BCR860 后台命令注入 (CVE-2023-3450) 某迈特 在特定场景下设置 Token 回调地址漏洞 8/9/2023 某恒明御运维审计与风险控制系统 service 任意用户添加漏洞 8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞(CVE-2023-34644) 8/9/2023 某恒明御安全网关 命令执行漏洞(CNVD-2023-03898)	8/9/2023	Exchange Server 远程代码执行漏洞
		(CVE-2023-38182)
(CVE-2023-3450) 8/9/2023	8/9/2023	某远 OA wpsAssistServlet 任意文件上传漏洞
	8/9/2023	某捷 RG-BCR860 后台命令注入
8/9/2023 某恒明御运维审计与风险控制系统 service 任意用户添加漏洞 8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644) 8/9/2023 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898)		(CVE-2023-3450)
用户添加漏洞	8/9/2023	某迈特 在特定场景下设置 Token 回调地址漏洞
8/9/2023 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644)	8/9/2023	某恒明御运维审计与风险控制系统 service 任意
(CVE-2023-34644) 8/9/2023		用户添加漏洞
8/9/2023 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898)	8/9/2023	某捷 EWEB 管理系统远程代码注入漏洞
(CNVD-2023-03898)		(CVE-2023-34644)
	8/9/2023	某恒明御安全网关 命令执行漏洞
8/9/2023 某联达 OA SQL 注入漏洞		(CNVD-2023-03898)
	8/9/2023	某联达 OA SQL 注入漏洞

8/9/2023	某联达 OA 后台文件上传漏洞
8/9/2023	某康综合安防管理平台 files 任意文件上传漏洞
8/9/2023	某康综合安防管理平台 report 任意文件上传漏
	洞
8/9/2023	某神 SecGate 3600 防火墙 obj_app_upfile
	任意文件上传漏洞
8/9/2023	某神 SecSSL 3600 安全接入网关系统 任意密
	码修改漏洞
8/9/2023	某得 SRM tomcat.jsp 登录绕过漏洞
8/9/2023	某景云终端安全管理系统 login SQL 注入漏洞
8/10/2023	某友移动某系统 uploadApk.do 任意文件上传
	漏洞
8/10/2023	飞某联 OA 文件读取漏洞
8/10/2023	某联达 oa 后台文件上传漏洞
8/10/2023	某石网科 LMS 系统命令执行漏洞
8/10/2023	某翼云网页防篡改系统命令执行漏洞
8/10/2023	某麒麟堡垒机系统 SQL 注入漏洞
8/10/2023	某远 OA 系统命令执行漏洞
8/10/2023	某远 OA 系统 V5-V6 模块命令执行漏洞
8/10/2023	某石网科 EDR 系统 PHP 模块命令执行漏洞
8/10/2023	某华三 NX54 系统 web 模块信息泄露漏洞
8/10/2023	某捷 EG 易网关系统命令执行漏洞

8/10/2023	某华三 虚拟授权管理系统系统命令执行漏洞
8/10/2023	某华三 虚拟授权管理系统系统 web 模块命令
	执行漏洞
8/10/2023	某华三 综合日志审计平台系统命令执行漏洞
8/10/2023	某福迪 堡垒机系统 web 模块 SQL 注入漏洞
8/10/2023	某盟 SAS 堡垒机 localuser.php 任意用户登录
	漏洞
8/10/2023	某盟 SAS 堡垒机 GetFile 任意文件读取漏洞
8/10/2023	某盟 SAS 堡垒机 Exec 远程命令执行漏洞
8/10/2023	某康 综合安防管理平台 env 信息泄漏漏洞
8/10/2023	某恒明御运维审计与风险控制系统 xmlrpc.sock
	任意用户添加漏洞
8/10/2023	某捷 NBR 路由器 fileupload.php 任意文件上
	传漏洞
8/10/2023	某华三 Magic CVE-2023-34928 远程代码执
	行漏洞
8/10/2023	某稀路由器命令执行漏洞
8/10/2023	某达 OA getdata 远程代码执行漏洞
8/10/2023	某帆 OA ioRepPicAdd 前台任意文件上传漏洞
8/10/2023	某思 OA wap.do SQL 注入漏洞
8/10/2023	某思 OA wap.do 任意文件下载漏洞