天融信脆弱性扫描与管理系统安全评估报告-系统综述报表

1. 综述信息

本次扫描摘要信息如下：存活主机1个，其中非常危险主机数1个、比较危险主机数0个、比较安全主机数0个、非常安全主机数0个。扫描总漏洞数10个，其中高危漏洞5个、中危漏洞1个、低危漏洞0个、信息漏洞4个。脆弱账号0个。cifs、ftp、ms-wbt-server、others、www位列服务漏洞数前五位。others位列应用漏洞数前五位。Windows Server 2008 R2 Standard 7601 Service Pack 1位列操作系统漏洞数前五位。

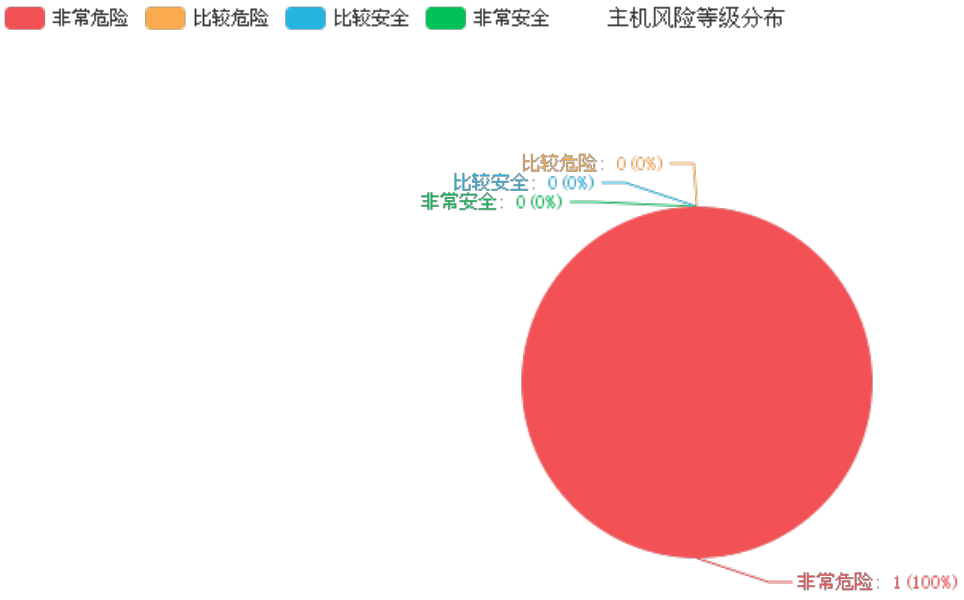
1.1任务信息

网络风险值	非常危险(8.4分)

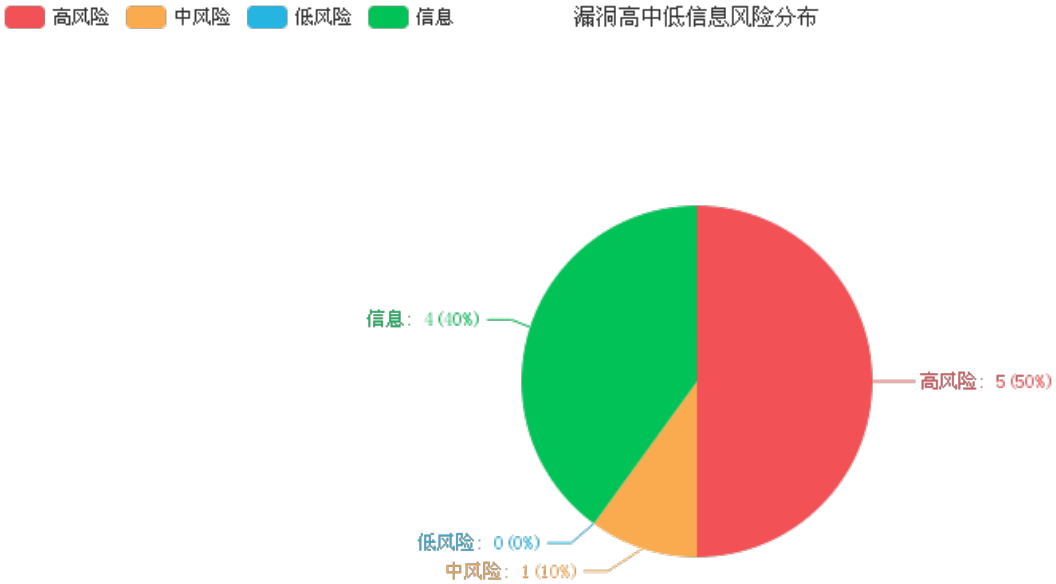
任务名称	高危资产单独评估	扫描引擎	本地
任务类型	系统任务	脆弱账号	0
任务耗时	2分钟16秒	主机统计	存活主机：1 已扫描主机：1 未扫描主机：0 主机总数：1
扫描器系统版本	v3.262209.1154_RSAS.1_V		
插件库版本	vas-sys-V1.1S01A01P00-2023		
时间统计	开始时间：2024-04-04 21:25:11 结束时间：2024-04-04 21:27:27		
漏洞风险	高危漏洞：5 中危漏洞：1 低危漏洞：0 信息漏洞：4	主机风险	非常危险主机：1 比较危险主机：0 比较安全主机：0 非常安全主机：0

1.2风险分布

1.2.1主机风险分布



1.2.2漏洞风险分布



1.3资产综述

1.3.1操作系统

操作系统	主机数量	比率
Windows Server 2008 R2 Standard 7601 Service Pack 1	1	100.0%
合计	1	100%

2. 主机信息

2.1主机风险等级列表

IP地址	主机名	操作系统	漏洞风险（个）					检查合规（个）				主机风险评估分
			高	中	低	信息	总计	不合规	异常	合规	总计	
192.168.2.44	WIN-RDUDODI4BAJ	Windows Server 2008 R2 Standard 7601 Service Pack 1	5	1	0	4	10	0	0	0	0	8.4
合计			5	1	0	4	10	0	0	0	0	

3. 漏洞信息

3.1漏洞分布

3.1.1 系统漏洞分布

漏洞类别： 高风险[5] 中风险[1] 低风险[0] 信息[4]

漏洞名称	Microsoft Windows SMB 输入验证错误漏洞 (CVE-2017-0143) 【原理扫描】
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	Starting Nmap 7.70 (https://nmap.org) at 2024-04-04 13:26 utc Nmap scan report for 192.168.2.44 Host is up (0.00026s latency). PORT STATE SERVICE 445/tcp open microsoft-ds MAC Address: 00:0C:29:6C:D0:1E (VMware) Host script results: | smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0143 | Risk factor: HIGH | A critical remote code execution vulnerability exists in Microsoft SMBv1 | servers (ms17-010). | | Disclosure date: 2017-03-14 | References: | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
漏洞描述	Microsoft Windows和Microsoft Windows Server都是美国微软（Microsoft）公司的产品。Microsoft Windows是一套个人设备使用的操作系统。Microsoft Windows Server是一套服务器操作系统。Server Message Block（SMB）Server是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。\nMicrosoft Windows中的SMBv1服务器存在远程代码执行漏洞。远程攻击者可借助特制的数据包利用该漏洞执行任意代码。以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
解决办法	厂商补丁：\n\nMicrosoft\n---------\nMicrosoft已经为此发布了一个安全公告（MS17-010）以及相应补丁:\nMS17-010: Microsoft Windows SMB 服务器安全更新 (4013389). \n链接：http://technet.microsoft.com/security/bulletin/MS17-010
威胁分值	8.1
发现日期	2017-03-28
发布日期	2017-03-28
TVID编号	TVID-201700-498155
CVE编号	CVE-2017-0143
CNNVD编号	CNNVD-201703-726
CNCVE编号	CNCVE-20170143
MS编号	
CNVD编号	
CVSS评分	8.1
BUGTRAQ	
影响的版本	以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
相关连接	https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

漏洞名称	Microsoft Windows SMB 输入验证错误漏洞 (CVE-2017-0144) 【原理扫描】
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	Starting Nmap 7.70 (https://nmap.org) at 2024-04-04 13:26 utc Nmap scan report for 192.168.2.44 Host is up (0.00026s latency). PORT STATE SERVICE 445/tcp open microsoft-ds MAC Address: 00:0C:29:6C:D0:1E (VMware) Host script results: | smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0143 | Risk factor: HIGH | A critical remote code execution vulnerability exists in Microsoft SMBv1 | servers (ms17-010). | | Disclosure date: 2017-03-14 | References: | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
漏洞描述	Microsoft Windows和Microsoft Windows Server都是美国微软（Microsoft）公司的产品。Microsoft Windows是一套个人设备使用的操作系统。Microsoft Windows Server是一套服务器操作系统。Server Message Block（SMB）Server是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。\nMicrosoft Windows中的SMBv1服务器存在远程代码执行漏洞。远程攻击者可借助特制的数据包利用该漏洞执行任意代码。以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
解决办法	厂商补丁：\n\nMicrosoft\n---------\nMicrosoft已经为此发布了一个安全公告（MS17-010）以及相应补丁:\nMS17-010: Microsoft Windows SMB 服务器安全更新 (4013389). \n链接：http://technet.microsoft.com/security/bulletin/MS17-010
威胁分值	8.1
发现日期	2017-03-28
发布日期	2017-03-28
TVID编号	TVID-201700-498156
CVE编号	CVE-2017-0144
CNNVD编号	CNNVD-201703-725
CNCVE编号	CNCVE-20170144
MS编号	
CNVD编号	
CVSS评分	8.1
BUGTRAQ	
影响的版本	以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
相关连接	https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

漏洞名称	Microsoft Windows SMB 输入验证错误漏洞 (CVE-2017-0145) 【原理扫描】
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	Starting Nmap 7.70 (https://nmap.org) at 2024-04-04 13:26 utc Nmap scan report for 192.168.2.44 Host is up (0.00026s latency). PORT STATE SERVICE 445/tcp open microsoft-ds MAC Address: 00:0C:29:6C:D0:1E (VMware) Host script results: | smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0143 | Risk factor: HIGH | A critical remote code execution vulnerability exists in Microsoft SMBv1 | servers (ms17-010). | | Disclosure date: 2017-03-14 | References: | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
漏洞描述	Microsoft Windows和Microsoft Windows Server都是美国微软（Microsoft）公司的产品。Microsoft Windows是一套个人设备使用的操作系统。Microsoft Windows Server是一套服务器操作系统。Server Message Block（SMB）Server是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。\nMicrosoft Windows中的SMBv1服务器存在远程代码执行漏洞。远程攻击者可借助特制的数据包利用该漏洞执行任意代码。以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
解决办法	厂商补丁：\n\nMicrosoft\n---------\nMicrosoft已经为此发布了一个安全公告（MS17-010）以及相应补丁:\nMS17-010: Microsoft Windows SMB 服务器安全更新 (4013389). \n链接：http://technet.microsoft.com/security/bulletin/MS17-010
威胁分值	8.1
发现日期	2017-03-28
发布日期	2017-03-28
TVID编号	TVID-201700-498157
CVE编号	CVE-2017-0145
CNNVD编号	CNNVD-201703-724
CNCVE编号	CNCVE-20170145
MS编号	
CNVD编号	
CVSS评分	8.1
BUGTRAQ	
影响的版本	以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
相关连接	https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

漏洞名称	Microsoft Windows SMB 输入验证错误漏洞 (CVE-2017-0146) 【原理扫描】
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	Starting Nmap 7.70 (https://nmap.org) at 2024-04-04 13:26 utc Nmap scan report for 192.168.2.44 Host is up (0.00026s latency). PORT STATE SERVICE 445/tcp open microsoft-ds MAC Address: 00:0C:29:6C:D0:1E (VMware) Host script results: | smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0143 | Risk factor: HIGH | A critical remote code execution vulnerability exists in Microsoft SMBv1 | servers (ms17-010). | | Disclosure date: 2017-03-14 | References: | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
漏洞描述	Microsoft Windows和Microsoft Windows Server都是美国微软（Microsoft）公司的产品。Microsoft Windows是一套个人设备使用的操作系统。Microsoft Windows Server是一套服务器操作系统。Server Message Block（SMB）Server是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。\nMicrosoft Windows中的SMBv1服务器存在远程代码执行漏洞。远程攻击者可借助特制的数据包利用该漏洞执行任意代码。以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
解决办法	厂商补丁：\n\nMicrosoft\n---------\nMicrosoft已经为此发布了一个安全公告（MS17-010）以及相应补丁:\nMS17-010: Microsoft Windows SMB 服务器安全更新 (4013389). \n链接：http://technet.microsoft.com/security/bulletin/MS17-010
威胁分值	8.1
发现日期	2017-03-28
发布日期	2017-03-28
TVID编号	TVID-201700-498158
CVE编号	CVE-2017-0146
CNNVD编号	CNNVD-201703-723
CNCVE编号	CNCVE-20170146
MS编号	
CNVD编号	
CVSS评分	8.1
BUGTRAQ	
影响的版本	以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
相关连接	https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

漏洞名称	Microsoft Windows SMB 输入验证错误漏洞 (CVE-2017-0148) 【原理扫描】
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	Starting Nmap 7.70 (https://nmap.org) at 2024-04-04 13:26 utc Nmap scan report for 192.168.2.44 Host is up (0.00026s latency). PORT STATE SERVICE 445/tcp open microsoft-ds MAC Address: 00:0C:29:6C:D0:1E (VMware) Host script results: | smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0143 | Risk factor: HIGH | A critical remote code execution vulnerability exists in Microsoft SMBv1 | servers (ms17-010). | | Disclosure date: 2017-03-14 | References: | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
漏洞描述	Microsoft Windows和Microsoft Windows Server都是美国微软（Microsoft）公司的产品。Microsoft Windows是一套个人设备使用的操作系统。Microsoft Windows Server是一套服务器操作系统。Server Message Block（SMB）Server是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。\nMicrosoft Windows中的SMBv1服务器存在远程代码执行漏洞。远程攻击者可借助特制的数据包利用该漏洞执行任意代码。以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
解决办法	厂商补丁：\n\nMicrosoft\n---------\nMicrosoft已经为此发布了一个安全公告（MS17-010）以及相应补丁:\nMS17-010: Microsoft Windows SMB 服务器安全更新 (4013389). \n链接：http://technet.microsoft.com/security/bulletin/MS17-010
威胁分值	8.1
发现日期	2017-03-28
发布日期	2017-03-28
TVID编号	TVID-201700-498160
CVE编号	CVE-2017-0148
CNNVD编号	CNNVD-201703-721
CNCVE编号	CNCVE-20170148
MS编号	
CNVD编号	
CVSS评分	8.1
BUGTRAQ	
影响的版本	以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
相关连接	https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

漏洞名称	Microsoft Windows SMB 信息泄露漏洞 (CVE-2017-0147) 【原理扫描】
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	Starting Nmap 7.70 (https://nmap.org) at 2024-04-04 13:26 utc Nmap scan report for 192.168.2.44 Host is up (0.00026s latency). PORT STATE SERVICE 445/tcp open microsoft-ds MAC Address: 00:0C:29:6C:D0:1E (VMware) Host script results: | smb-vuln-ms17-010: | VULNERABLE: | Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010) | State: VULNERABLE | IDs: CVE:CVE-2017-0143 | Risk factor: HIGH | A critical remote code execution vulnerability exists in Microsoft SMBv1 | servers (ms17-010). | | Disclosure date: 2017-03-14 | References: | https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ | https://technet.microsoft.com/en-us/library/security/ms17-010.aspx |_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143 Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
漏洞描述	Microsoft Windows是美国微软（Microsoft）公司发布的一系列操作系统。SMBv1 server是其中的一个服务器协议组件。\nMicrosoft Windows中的SMBv1服务器存在信息泄露漏洞。远程攻击者可借助特制的数据包利用该漏洞获取进程内存中的敏感信息。以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
解决办法	厂商补丁：\n\nMicrosoft\n---------\nMicrosoft已经为此发布了一个安全公告（MS17-010）以及相应补丁:\nMS17-010: Microsoft Windows SMB 服务器安全更新 (4013389). \n链接：http://technet.microsoft.com/security/bulletin/MS17-010
威胁分值	5.9
发现日期	2017-03-28
发布日期	2017-03-28
TVID编号	TVID-201700-498159
CVE编号	CVE-2017-0147
CNNVD编号	CNNVD-201703-722
CNCVE编号	CNCVE-20170147
MS编号	
CNVD编号	
CVSS评分	5.9
BUGTRAQ	
影响的版本	以下版本受到影响：Microsoft Windows Vista SP2，Windows Server 2008 SP2和R2 SP1，Windows 7 SP1，Windows 8.1，Windows Server 2012 Gold和R2，Windows RT 8.1，Windows 10 Gold，1511和1607，Windows Server 2016。
相关连接	https://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

漏洞名称	HTTP横幅
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Fri, 25 Jun 2021 06:21:31 GMT Accept-Ranges: bytes ETag: "2e6ddc568a69d71:0" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Thu, 04 Apr 2024 13:27:17 GMT Connection: close Content-Length: 689
漏洞描述	此脚本获取HTTP标题并在与此标题相关的KB中存储一些值。
解决办法	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商主页或参考网址以获取解决办法
威胁分值	0
发现日期	2017-02-21
发布日期	2018-06-01
TVID编号	TVID-202101-3805
CVE编号	
CNNVD编号	
CNCVE编号	
MS编号	
CNVD编号	
CVSS评分	0
BUGTRAQ	
影响的版本	
相关连接	NOXREF

漏洞名称	Microsoft远程桌面协议检测
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	
漏洞描述	支持Microsoft远程桌面协议（RDP）的服务正在此主机上运行。 远程桌面服务（以前称为终端服务）是Microsoft Windows（服务器和客户端版本）的组件之一，允许用户通过网络访问远程计算机上的应用程序和数据。
解决办法	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商主页或参考网址以获取解决办法
威胁分值	0
发现日期	2009-03-20
发布日期	2018-06-27
TVID编号	TVID-202101-11391
CVE编号	
CNNVD编号	
CNCVE编号	
MS编号	
CNVD编号	
CVSS评分	0
BUGTRAQ	
影响的版本	
相关连接	NOXREF

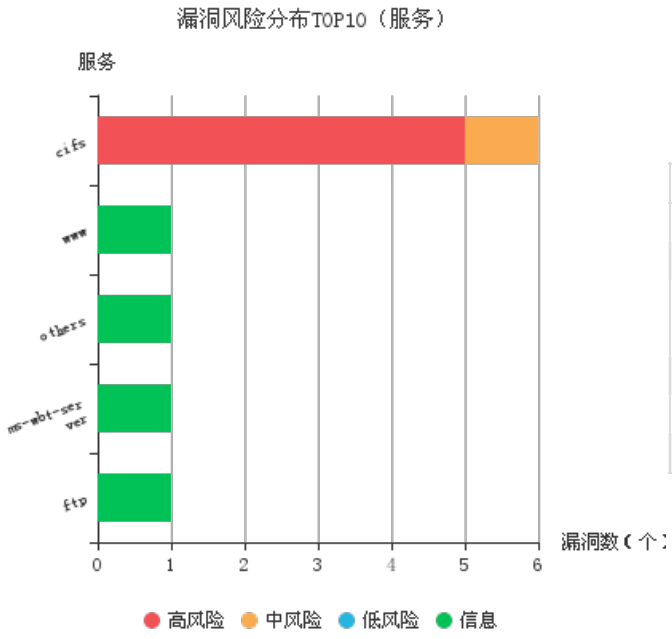
漏洞名称	已启用匿名FTP(CVE-1999-0497)
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	
漏洞描述	Nessus检测到远程主机上运行的FTP服务器允许匿名登录。因此，任何远程用户都可以连接到服务器并进行身份验证，而无需提供密码或唯一凭据。这允许用户访问FTP服务器提供的任何文件。
解决办法	Topvas建议您采取以下措施以降低威胁:\n\n如果并不需要开放匿名FTP服务，您应该禁止匿名帐号。\n\n* 在大多数的unix系统下，可以使用下列命令来禁止:\n # echo ftp >> /etc/ftpusers\n\n* 在Windows系统下，您可以在服务管理器中停止FTP服务，并将该服务的启动类型设\n 置为手动，或在“添加/删除应用程序”中将服务卸载。
威胁分值	0
发现日期	2021-04-29
发布日期	2021-04-29
TVID编号	TVID-199900-48179
CVE编号	CVE-1999-0497
CNNVD编号	
CNCVE编号	CNCVE-19990497
MS编号	
CNVD编号	
CVSS评分	0
BUGTRAQ	
影响的版本	
相关连接	NOXREF

漏洞名称	跟踪路由
影响主机个数	1
影响主机百分比	100.0%
出现次数	1
受影响的主机	192.168.2.44
检测详情	For your information, here is the traceroute from 192.168.2.15 to 192.168.2.44 : 192.168.2.15 192.168.2.44 Hop Count: 1
漏洞描述	进行了从扫描服务器到目标系统的跟踪路由。 此traceroute主要仅用于提供信息值。 在绝大多数情况下，它并不代表漏洞。 但是，如果显示的traceroute包含任何不应公开显示的私有地址，那么您需要纠正一个问题。
解决办法	阻止不需要的数据包逃离您的网络。
威胁分值	0
发现日期	2010-07-09
发布日期	2018-01-25
TVID编号	TVID-202101-3717
CVE编号	
CNNVD编号	
CNCVE编号	
MS编号	
CNVD编号	
CVSS评分	0
BUGTRAQ	
影响的版本	
相关连接	NOXREF

4. 风险类别

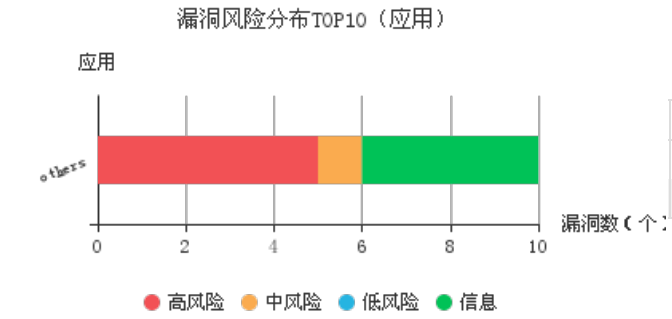
4.1漏洞风险类别

4.1.1服务分类



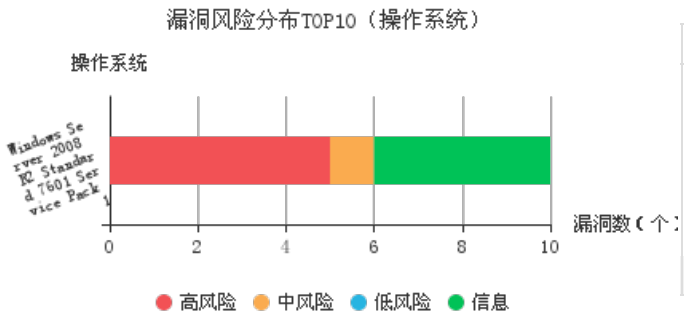
服务	高风险	中风险	低风险	信息	总计
cifs	5	1	0	0	6
ftp	0	0	0	1	1
ms-wbt-server	0	0	0	1	1
others	0	0	0	1	1
www	0	0	0	1	1
合计	5	1	0	4	10

4.1.2应用分类



应用	高风险	中风险	低风险	信息	总计
others	5	1	0	4	10
合计	5	1	0	4	10

4.1.3操作系统分类



操作系统	高风险	中风险	低风险	信息	总计
Windows Server 2008 R2 Standard 7601 Service Pack 1	5	1	0	4	10
合计	5	1	0	4	10

5. 脆弱账号

5.1应用程序脆弱账号

IP地址	用户名	密码	应用类型	端口

6. 参考标准

6.1单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <=10	攻击者可远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	1 <= 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息或读取系统文件和数据。
信息	0 <= 漏洞风险值 < 1	攻击者可以获取某系统或者服务的信息。

说明：

漏洞的风险值兼容CVSS评分标准。

6.2主机风险等级评定标准

主机风险等级	主机风险评估分区域
非常危险	7.0 <= 主机风险评估分 <= 10.0
比较危险	5.0 <= 主机风险评估分 < 7.0
比较安全	2.0 <= 主机风险评估分 < 5.0
非常安全	0.0 <= 主机风险评估分 < 2.0

说明：

1. 按照脆弱性扫描与管理系统的主机风险评估模型计算主机风险评估分。根据得到的主机风险评估分参考“主机风险等级评定标准”标识主机风险等级。
2. 将主机风险等级按照风险评估分的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种主机风险等级。
3. 用户可以根据自己的需要修订主机风险等级中的主机风险评估分范围。

6.3网络风险等级评定标准

网络风险等级	网络风险值区域
非常危险	7.0 <= 网络风险值 <= 10.0
比较危险	5.0 <= 网络风险值 < 7.0
比较安全	2.0 <= 网络风险值 < 5.0
非常安全	0.0 <= 网络风险值 < 2.0

说明：

1. 按照脆弱性扫描与管理系统的网络风险评估模型计算该网络风险值。根据得到的网络风险值参考“网络风险等级评定标准”标识网络风险等级。
2. 将网络风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种网络风险等级。

6.4安全建议

据市场研究公司 Gartner 研究报告称"实施漏洞管理的企业会避免近 90% 的攻击"。可以看出，及时的漏洞修补可以在一定程度上防止病毒、攻击者的威胁。

脆弱性扫描与管理系统建议对存在漏洞的主机参考附件中提出的解决方案进行漏洞修补、安全增强。

- 建议所有 Windows 系统使用"Windows Update"进行更新。
- 对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。
- 对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。
- 对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的。
- 对于UNIX系统订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安装、停止服务等。
- 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。
- 建议采用脆弱性扫描与管理系统定期对网络进行评估，真正做到未雨绸缪。

脆弱性扫描与管理系统建议对存在不合规检查项的主机参考对应的检查点详情中提出的调整方案和标准值进行修正。

6.5联系我们

公司：北京天融信公司
网址：www.topsec.com.cn
热线：8610-82776666
传真：8610-82776677
地址：北京市海淀区上地东路1号华控大厦