1章节目录

2 主机详细

2.1 主机10.34.100.150

资产名称	--
所属部门	--
资产类型	--
资产价值	--
NetBios名	WIN-NFA8MEV4V9A
netbios域名/工作组	WORKGROUP
保护等级	--
主机名	WIN-NFA8MEV4V9A(08:94:ef:6e:46:5f)
主机风险状态	极度危险
操作系统信息	Microsoft Windows

序号	猜测类型	用户名	密码(隐藏)	描述
N/A				

端口/漏洞列表

0__其他协议__其他服务				
序号	危险级别	漏洞编号	漏洞名称	返回信息
1	信息	001E93A6	ICMP权限许可和访问控制漏洞CVE-1999-0524	
2	信息	0x1ebc5e	目标主机允许Traceroute探测	

7__UDP__未知服务				
序号	危险级别	漏洞编号	漏洞名称	返回信息

3	信息	001E97EB	回声服务运行漏洞CVE-1999-0635	
4	信息	0xb2d36c71	目标主机运行着ECHO服务	

9__TCP__discard				
序号	危险级别	漏洞编号	漏洞名称	返回信息
5	低危险	00300AB	远程主机DISCARD服务正在运行	

80__TCP__http				
序号	危险级别	漏洞编号	漏洞名称	返回信息
6	高危险	00E713C	Microsoft Windows HTTP.sys 远程执行代码漏洞(CVE-2015-1635)【原理扫描】	
7	信息	0x0013026A	检测到目标主机IIS服务正在运行	IIS Webserver:[0: 'IIS/8.5', 1: '8.5']
8	信息	0x001303CC	检测到远程主机HTTP Server正在运行	
9	信息	0x1ebe9a	远程主机HTTP协议版本信息泄漏	
10	信息	0xb2d36ca2	通过HTTP获取目标主机的WWW服务信息	

137__TCP__未知服务				
序号	危险级别	漏洞编号	漏洞名称	返回信息
11	信息	0x001303E2	可通过NetBIOS名字服务端口远程获取系统信息	

8080__TCP__http-proxy				
序号	危险级别	漏洞编号	漏洞名称	返回信息
12	高危险	0x1eb9b5	Apache Tomcat 远程代码执行漏洞(CVE-2016-8735)	

13	高危险	0x1ebc91	Apache Tomcat Commons Fileupload 拒绝服务漏洞(CVE-2016-3092)	
14	高危险	0x1ebc96	Apache Tomcat httpoxy 安全漏洞(CVE-2016-5388)	
15	高危险	0x1ebc97	Apache Tomcat 安全绕过漏洞(CVE-2016-6816)	
16	高危险	0xb2d36c82	Apache Tomcat 安全漏洞(CVE-2017-5648)	
17	高危险	0xb2d36fa6	Apache Tomcat Default Servlet 安全漏洞(CVE-2017-5664)	
18	高危险	0xb2d370f	Tomcat 远程代码执行漏洞(CVE-2017-12615)	
19	高危险	0xb2d370f	Tomcat 信息泄露漏洞(CVE-2017-12616)	
20	高危险	0xb2d371fb	Apache Tomcat 安全漏洞(CVE-2017-12617)	
21	高危险	0xb2d371fc	Apache Tomcat 安全漏洞(CVE-2017-5647)	
22	高危险	0xb2d374f8	Apache Tomcat 安全漏洞(CVE-2018-1304)	
23	高危险	0xb2d374f9	Apache Tomcat 安全漏洞(CVE-2018-1305)	
24	高危险	0xb2d3bf65	Apache Tomcat CORS Filter 安全漏洞(CVE-2018-8014)	
25	高危险	0xb2d3c191	Apache Tomcat 安全漏洞(CVE-2019-0232)	
26	中危险	00AA0C13	Apache Tomcat 安全漏洞(CVE-2018-11784)	
27	中危险	00AA0C4F	Apache Tomcat 安全漏洞(CVE-2018-1336)	
28	中危险	00AA0DF8	Apache Tomcat 安全漏洞(CVE-2018-8034)	
29	中危险	0x1ebc66	Apache Tomcat 安全绕过漏洞(CVE-2016-6796)	
30	中危险	0x1ebc67	Apache Tomcat 安全漏洞(CVE-2016-6794)	

31	中危险	0x1ebc68	Apache Tomcat 安全绕过漏洞(CVE-2016-5018)	
32	中危险	0x1ebc69	Apache Tomcat 信息泄露漏洞(CVE-2016-0762)	
33	中危险	0x1ebc6a	Apache Tomcat 安全漏洞(CVE-2016-6797)	
34	中危险	0x1ebc74	Apache Tomcat 信息泄露漏洞(CVE-2016-8745)	
35	中危险	0xb2d36fe7	Apache Tomcat CORS Filter 安全漏洞(CVE-2017-7674)	
36	信息	0x0013048C	检测到目标主机Apache Tomcat正在运行	Apache Tomcat Version:7.0.69

7__TCP__echo
13__TCP__daytime
17__TCP__qotd
19__TCP__chargen
42__TCP__nameserver
81__TCP__hosts2-ns
137__UDP__netbios-ns
1801__TCP__msmq
2103__TCP__zephyr-clt
2105__TCP__eklogin
2107__TCP__msmq-mgmt
5985__TCP__wsman
8009__TCP__ajp13
9999__TCP__abyss
40002__TCP__unknown
49152__TCP__unknown

49153__TCP__unknown
49154__TCP__unknown
49155__TCP__unknown
49157__TCP__unknown
49158__TCP__unknown
49160__TCP__unknown
49175__TCP__unknown

2.2 漏洞详细

【1】Apache Tomcat 远程代码执行漏洞(CVE-2016-8735)	
漏洞编号	0x1eb9b5
漏洞类型	WEB类
危险级别	高危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M11版本， Apache Tomcat 8.5.0至8.5.6版本， Apache Tomcat 8.0.0.RC1至8.0.38版本， Apache Tomcat 7.0.0至7.0.72版本， Apache Tomcat 6.0.0至6.0.47版本。
CVSS分值	9.8
bugtraq编号	
CVE编号	CVE-2016-8735
CNCVE编号	CNCVE-20168735
国家漏洞库编号	CNNVD-201611-609
CNVD编号	0
简单描述	Apache Tomcat 远程代码执行漏洞

详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在代码执行漏洞。远程攻击者可利用该漏洞在受影响应用程序上下文中执行任意代码。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M11版本，Apache Tomcat 8.5.0至8.5.6版本，Apache Tomcat 8.0.0.RC1至8.0.38版本，Apache Tomcat 7.0.0至7.0.72版本，Apache Tomcat 6.0.0至6.0.47版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://tomcat.apache.org/security-6.htmlhttp://tomcat.apache.org/security-7.htmlhttp://tomcat.apache.org/security-8.htmlhttp://tomcat.apache.org/security-9.html
参考网址	链接:http://www.securityfocus.com/bid/94463

【2】Apache Tomcat Commons Fileupload 拒绝服务漏洞(CVE-2016-3092)	
漏洞编号	0x1ebc91
漏洞类型	Apache类
危险级别	高危险
影响平台	The MultipartStream classApache Commons Fileupload before 1.3.2 usedApache Tomcat 7.x before 7.0.70 8.x before 8.0.36 8.5.x before 8.5.3 and 9.x before 9.0.0.M7 and other products
CVSS分值	7.5
bugtraq编号	
CVE编号	CVE-2016-3092
CNCVE编号	CNCVE-20163092
国家漏洞库编号	CNNVD-201606-555
CNVD编号	0
简单描述	Apache Tomcat Commons Fileupload 拒绝服务漏洞
详细描述	Apache Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Commons FileUpload是其中的一个可将文件上传到Servlet和Web应用程序的软件包组件。;Apache Tomcat的Apache Commons Fileupload 1.3.2之前版本中存在安全漏洞。远程攻击者可借助较长的边界字符串利用该漏洞造成拒绝服务（CPU消耗）。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0M6版本，8.5.0版本至8.5.2版本，8.0.0.RC1版本至8.0.35版本，7.0.0版本至7.0.69版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://tomcat.apache.org/security-7.htmlhttp://tomcat.apache.org/security-8.htmlhttp://tomcat.apache.org/security-9.html

参考网址	链接:http://svn.apache.org/viewvc?view=revision&revision=1743722 链接:http://svn.apache.org/viewvc?view=revision&revision=1743480 链接:https://bugzilla.redhat.com/show_bug.cgi?id=1349468 链接:http://jvn.jp/en/jp/JVN89379547/index.html 链接:http://tomcat.apache.org/security-8.html 链接:http://jvndb.jvn.jp/jvndb/JVNDB-2016-000121 链接:http://mail-archives.apache.org/mod_mbox/commons-dev/201606.mbox/%3CCAF8HOZ%2BPq2QH8RnxBuJyoK1dOz6jrTiQypAC%2BH8g6oZkBg%2BCxg%40mail.gmail.com%3E 链接:http://svn.apache.org/viewvc?view=revision&revision=1743738 链接:http://tomcat.apache.org/security-9.html 链接:http://tomcat.apache.org/security-7.html 链接:http://svn.apache.org/viewvc?view=revision&revision=1743742 链接:http://www.auscert.org.au/./render.html?it=36134 链接：http://www.nsfocus.net/vulndb/33932

【3】Apache Tomcat httpoxy 安全漏洞(CVE-2016-5388)	
漏洞编号	0x1ebc96
漏洞类型	WEB类
危险级别	高危险
影响平台	Apache Tomcat 7.x through 7.0.70 and 8.x through 8.5.4
CVSS分值	8.1
bugtraq编号	
CVE编号	CVE-2016-5388
CNCVE编号	CNCVE-20165388
国家漏洞库编号	CNNVD-201607-541
CNVD编号	0
简单描述	Apache Tomcat httpoxy 安全漏洞
详细描述	Apache Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat 8.5.4及之前的版本中存在安全漏洞，该漏洞源于程序没有解决RFC 3875模式下的命名空间冲突。程序没有正确处理来自HTTP_PROXY环境变量中不可信客户端数据应用程序。远程攻击者借助HTTP请求中特制的Proxy header消息利用该漏洞实施中间人攻击，指引服务器发送连接到任意主机。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://www.apache.org/security/asf-httpoxy-response.txt
参考网址	链接:https://www.apache.org/security/asf-httpoxy-response.txt 链接:http://www.kb.cert.org/vuls/id/797896 链接:https://httpoxy.org/

【4】Apache Tomcat 安全绕过漏洞(CVE-2016-6816)	
漏洞编号	0x1ebc97
漏洞类型	WEB类
危险级别	高危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M11版本，8.5.0至8.5.6版本，8.0.0.RC1至8.0.38版本，7.0.0至7.0.72版本，6.0.0至6.0.47版本。
CVSS分值	7.1
bugtraq编号	
CVE编号	CVE-2016-6816
CNCVE编号	CNCVE-20166816
国家漏洞库编号	CNNVD-201611-610
CNVD编号	0
简单描述	Apache Tomcat 安全绕过漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在安全绕过漏洞。攻击者可利用该漏洞绕过安全限制，执行未授权操作。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M11版本，8.5.0至8.5.6版本，8.0.0.RC1至8.0.38版本，7.0.0至7.0.72版本，6.0.0至6.0.47版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39
参考网址	链接:http://www.securityfocus.com/bid/94461

【5】Apache Tomcat 安全漏洞(CVE-2017-5648)	
漏洞编号	0xb2d36c82
漏洞类型	WEB类
危险级别	高危险

影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0.M17版本，8.5.0版本至8.5.11版本，8.0.0.RC1版本至8.0.41版本，7.0.0版本至7.0.75版本。
CVSS分值	9.1
bugtraq编号	
CVE编号	CVE-2017-5648
CNCVE编号	CNCVE-20175648
国家漏洞库编号	CNNVD-201704-593
CNVD编号	
简单描述	Apache Tomcat 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在安全漏洞。攻击者可利用该漏洞访问或更改其他Web应用程序的信息。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0.M17版本，8.5.0版本至8.5.11版本，8.0.0.RC1版本至8.0.41版本，7.0.0版本至7.0.75版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://bz.apache.org/bugzilla/show_bug.cgi?id=60718
参考网址	链接:http://www.securityfocus.com/bid/97530 链接:https://lists.apache.org/thread.html/d0e00f2e147a9e9b13a6829133092f349b2882bf6860397368a52600@%3Cannounce.tomcat.apache.org%3E

【6】Apache Tomcat Default Servlet 安全漏洞(CVE-2017-5664)	
漏洞编号	0xb2d36fa6
漏洞类型	WEB类
危险级别	高危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0.M20版本，8.5.0版本至8.5.14版本，8.0.0.RC1版本至8.0.43版本，7.0.0版本至7.0.77版本。
CVSS分值	7.5
bugtraq编号	
CVE编号	CVE-2017-5664
CNCVE编号	CNCVE-20175664
国家漏洞库编号	CNNVD-201706-192

CNVD编号	
简单描述	Apache Tomcat Default Servlet 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Default Servlet是其中的一个对静态资源进行处理的类。;Apache Tomcat中的Default Servlet存在安全漏洞。攻击者可利用该漏洞绕过安全限制，执行未授权的操作。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0.M20版本，8.5.0版本至8.5.14版本，8.0.0.RC1版本至8.0.43版本，7.0.0版本至7.0.77版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://tomcat.apache.org/security-7.htmlhttp://tomcat.apache.org/security-8.htmlhttp://tomcat.apache.org/security-9.html
参考网址	链接 :https://lists.apache.org/thread.html/a42c48e37398d76334e17089e43ccab945238b8b7896538478d76066@%3Cannounce.tomcat.apache.org%3E

【7】Tomcat 远程代码执行漏洞(CVE-2017-12615)	
漏洞编号	0xb2d370f
漏洞类型	WEB类
危险级别	高危险
影响平台	Apache Tomcat 7.0.0 to 7.0.79
CVSS分值	10.0
bugtraq编号	
CVE编号	CVE-2017-12615
CNCVE编号	
国家漏洞库编号	CNNVD-201709-899
CNVD编号	
简单描述	攻击者可以通过精心构造的攻击请求，向用户Tomcat服务器上传恶意 JSP 文件，通过上传的 JSP 文件，可在用户服务器上执行任意代码。
详细描述	When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/8fcb1e2d5895413abcf266f011b9918ae03e0b7daceb118ffbf23f8c@%3Cannounce.tomcat.apache.org%3E
参考网址	

【8】Tomcat 信息泄露漏洞(CVE-2017-12616)	
漏洞编号	0xb2d370f
漏洞类型	WEB类
危险级别	高危险
影响平台	Apache Tomcat 7.0.0 to 7.0.80
CVSS分值	8.0
bugtraq编号	
CVE编号	CVE-2017-12616
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	Tomcat信息泄露漏洞
详细描述	When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request.
修补建议	请及时升级Tomcat服务器至7.0.81及更高版本
参考网址	

【9】Apache Tomcat 安全漏洞(CVE-2017-12617)	
漏洞编号	0xb2d371fb
漏洞类型	WEB类
危险级别	高危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0版本，8.5.0版本至8.5.22版本，8.0.0.RC1版本至8.0.46版本，7.0.0版本至7.0.81版本。
CVSS分值	8.1

bugtraq编号	
CVE编号	CVE-2017-12617
CNCVE编号	CNCVE-201712617
国家漏洞库编号	CNNVD-201709-1092
CNVD编号	
简单描述	Apache Tomcat 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat中存在安全漏洞。攻击者可通过发送特制的请求利用该漏洞向服务器上传JSP文件，并执行文件中包含的代码。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0版本，8.5.0版本至8.5.22版本，8.0.0.RC1版本至8.0.46版本，7.0.0版本至7.0.81版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bz.apache.org/bugzilla/show_bug.cgi?id=61542
参考网址	参考网址;来源:BID;链接:http://www.securityfocus.com/bid/100954;;来源:MLIST;链接:https://lists.apache.org/thread.html/3fd341a604c4e9eab39e7eaabbbac39c30101a022acc11dd09d7ebcb@%3Cannounce.tomcat.apache.org%3E

【10】Apache Tomcat 安全漏洞(CVE-2017-5647)	
漏洞编号	0xb2d371fc
漏洞类型	WEB类
危险级别	高危险
影响平台	Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52
CVSS分值	7.5
bugtraq编号	
CVE编号	CVE-2017-5647
CNCVE编号	CNCVE-20175647
国家漏洞库编号	CNNVD-201704-862
CNVD编号	
简单描述	Apache Tomcat 安全漏洞

详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat中的pipelined请求的处理过程存在安全漏洞。攻击者可利用该漏洞读取其他请求的数据。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0.M18版本，8.5.0版本至8.5.12版本，8.0.0.RC1版本至8.0.42版本，7.0.0版本至7.0.76版本，6.0.0版本至6.0.52版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E
参考网址	参考网址;来源:MLIST;链接:https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E

【11】Apache Tomcat 安全漏洞(CVE-2018-1304)	
漏洞编号	0xb2d374f8
漏洞类型	Apache类
危险级别	高危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1到9.0.4版本，8.5.0版本到8.5.27版本，8.0.0.RC1版本至8.0.49版本，7.0.0版本至7.0.84版本。
CVSS分值	8.3
bugtraq编号	
CVE编号	CVE-2018-1304
CNCVE编号	
国家漏洞库编号	CNNVD-201802-668
CNVD编号	
简单描述	Apache Tomcat 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat中存在安全漏洞。攻击者可利用该漏洞访问受限制的Web应用程序资源。以下版本受到影响：Apache Tomcat 9.0.0.M1到9.0.4版本，8.5.0版本到8.5.27版本，8.0.0.RC1版本至8.0.49版本，7.0.0版本至7.0.84版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/b1d7e2425d6fd2cebed40d318f9365b44546077e10949b01b1f8a0fb@%3Cannounce.tomcat.apache.org%3E

参考网址	参考网址;来源:mail-archives.apache.org;链接:http://mail-archives.apache.org/mod_mbox/www-announce/201802.mbox/%3C2a8f2292-2aee-d8fa-9ccc-d1f9b20d0eed%40apache.org%3E

【12】Apache Tomcat 安全漏洞(CVE-2018-1305)	
漏洞编号	0xb2d374f9
漏洞类型	Apache类
危险级别	高危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1到9.0.4版本，8.5.0版本到8.5.27版本，8.0.0.RC1版本至8.0.49版本，7.0.0版本至7.0.84版本。
CVSS分值	8.3
bugtraq编号	
CVE编号	CVE-2018-1305
CNCVE编号	
国家漏洞库编号	CNNVD-201802-564
CNVD编号	
简单描述	Apache Tomcat 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat中存在安全漏洞。攻击者可利用该漏洞访问受限制的Web应用程序资源。以下版本受到影响：Apache Tomcat 9.0.0.M1到9.0.4版本，8.5.0版本到8.5.27版本，8.0.0.RC1版本至8.0.49版本，7.0.0版本至7.0.84版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/d3354bb0a4eda4acc0a66f3eb24a213fdb75d12c7d16060b23e65781@%3Cannounce.tomcat.apache.org%3E
参考网址	参考网址;来源:MISC;链接:https://lists.apache.org/thread.html/d3354bb0a4eda4acc0a66f3eb24a213fdb75d12c7d16060b23e65781@%3Cannounce.tomcat.apache.org%3E

【13】Apache Tomcat CORS Filter 安全漏洞(CVE-2018-8014)	
漏洞编号	0xb2d3bf65
漏洞类型	Apache类
危险级别	高危险

影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.8版本，8.5.0版本至8.5.31版本，8.0.0.RC1版本至8.0.52版本，7.0.41版本至7.0.88版本
CVSS分值	7.5
bugtraq编号	
CVE编号	CVE-2018-8014
CNCVE编号	CNCVE-20188014
国家漏洞库编号	CNNVD-201805-475
CNVD编号	
简单描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。CORS Filter是其中的一个提供跨源资源共享功能的组件。Apache Tomcat中的CORS Filter的默认配置存在安全漏洞。目前尚无此漏洞的相关信息，请随时关注CNNVD或厂商公告。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.8版本，8.5.0版本至8.5.31版本，8.0.0.RC1版本至8.0.52版本，7.0.41版本至7.0.88版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/fbfb713e4f8a4c0f81089b8945082801134359380 0cae3fb629192b1@%3Cannounce.tomcat.apache.org%3E
参考网址	URL:https://lists.apache.org/thread.html/fbfb713e4f8a4c0f81089b8945082801134359380 0cae3fb629192b1@%3Cannounce.tomcat.apache.org%3E,Source:lists.apache.org;URL:https://lists.apache.org/thread.html/fbfb713e4f8a4c0f81089b8945082801134359380 0cae3fb629192b1@%3Cannounce.tomcat.apache.org%3Ehttp://tomcat.apache.org/security-7.html,Source:tomcat.apache.org;URL:https://lists.apache.org/thread.html/fbfb713e4f8a4c0f81089b8945082801134359380 0cae3fb629192b1@%3Cannounce.tomcat.apache.org%3Ehttp://tomcat.apache.org/security-7.htmlhttp://tomcat.apache.org/security-9.html,Source:tomcat.apache.org;URL:https://lists.apache.org/thread.html/fbfb713e4f8a4c0f81089b8945082801134359380 0cae3fb629192b1@%3Cannounce.tomcat.apache.org%3Ehttp://tomcat.apache.org/security-7.htmlhttp://tomcat.apache.org/security-9.htmlhttp://tomcat.apache.org/security-8.html,Source:tomcat.apache.org;

【14】Apache Tomcat 安全漏洞(CVE-2019-0232)	
漏洞编号	0xb2d3c191
漏洞类型	Apache类
危险级别	高危险

影响平台	Apache Tomcat 9.0.0.M1 to 9.0.17,8.5.0 to 8.5.39,7.0.0 to 7.0.93
CVSS分值	7.5
bugtraq编号	
CVE编号	CVE-2019-0232
CNCVE编号	CNCVE-20190232
国家漏洞库编号	CNNVD-201904-525
CNVD编号	
简单描述	Apache Tomcat中存在安全漏洞。攻击者可利用该漏洞运行代码。
详细描述	Apache Tomcat中存在安全漏洞。攻击者可利用该漏洞运行代码。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://mail-archives.apache.org/mod_mbox/www-announce/201904.mbox/%3C13d878ec-5d49-c348-48d4-25a6c81b9605@apache.org%3E
参考网址	

【15】Microsoft Windows HTTP.sys 远程执行代码漏洞(CVE-2015-1635)【原理扫描】	
漏洞编号	00E713C
漏洞类型	NT关键问题类
危险级别	高危险
影响平台	Microsoft Windows 7 SP1 Windows Server 2008 R2 SP1Windows 8 Windows 8.1 and Windows Server 2012 Gold and R2
CVSS分值	10.0
bugtraq编号	
CVE编号	CVE-2015-1635
CNCVE编号	CNCVE-20151635
国家漏洞库编号	CNNVD-201504-257
CNVD编号	CNVD-2015-02422
简单描述	Microsoft Windows HTTP.sys 远程执行代码漏洞

详细描述	使用Microsoft IIS 6.0以上版本的Microsoft Windows的HTTP协议堆栈(HTTP.sys)中存在远程执行代码漏洞，该漏洞源于HTTP.sys文件没有正确分析经特殊设计的HTTP请求。成功利用此漏洞的攻击者可以在系统帐户的上下文中执行任意代码。Microsoft Windows 7 SP1，Windows Server 2008 R2 SP1，Windows 8，Windows 8.1，Windows Server 2012 和 Windows Server 2012 R2。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://technet.microsoft.com/library/security/ms15-034
参考网址	URL:http://www.securitytracker.com/id/1032109

【16】Apache Tomcat 安全漏洞(CVE-2018-11784)	
漏洞编号	00AA0C13
漏洞类型	Apache类
危险级别	中危险
影响平台	Apache Tomcat versions 9.0.0.M1 to 9.0.11, 8.5.0 to 8.5.33 and 7.0.23 to 7.0.90
CVSS分值	5.0
bugtraq编号	
CVE编号	CVE-2018-11784
CNCVE编号	CNCVE-201811784
国家漏洞库编号	CNNVD-201810-135
CNVD编号	
简单描述	Apache Tomcat 安全漏洞(CVE-2018-11784)
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat 9.0.0.M1版本至9.0.11版本，8.5.0版本至8.5.33版本和7.0.23版本至7.0.90版本中的默认servlet存在开放重定向漏洞。攻击者可借助特制的URL利用该漏洞重定向用户至任意web站点。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/23134c9b5a23892a205dc140cdd8c9c0add233600f76b313dda6bd75@%3Cannounce.tomcat.apache.org%3E
参考网址	

【17】Apache Tomcat 安全漏洞(CVE-2018-1336)	
漏洞编号	00AA0C4F

漏洞类型	Apache类
危险级别	中危险
影响平台	Apache Tomcat &;=9.0.0.M9， &;=9.0.7Apache Tomcat &;=8.5.0， &;=8.5.30Apache Tomcat &;=8.0.0.RC1， &;=8.0.51Apache Tomcat &;=7.0.28， &;=7.0.86
CVSS分值	5.0
bugtraq编号	
CVE编号	CVE-2018-1336
CNCVE编号	CNCVE-20181336
国家漏洞库编号	CNNVD-201807-1991
CNVD编号	
简单描述	Apache Tomcat 安全漏洞(CVE-2018-1336)
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat中存在拒绝服务漏洞。远程攻击者可通过发送特制的数据利用该漏洞造成拒绝服务（无限循环）。以下版本受到影响：Apache Tomcat 9.0.0.M9版本至9.0.7版本，8.5.0版本至8.5.30版本，8.0.0.RC1版本至8.0.51版本，7.0.28版本至7.0.86版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://tomcat.apache.org/security-8.htmlhttp://tomcat.apache.org/security-9.html
参考网址	

【18】Apache Tomcat 安全漏洞(CVE-2018-8034)	
漏洞编号	00AA0DF8
漏洞类型	Apache类
危险级别	中危险
影响平台	Apache Tomcat 9.0.0.M1 Apache Tomcat &;=7.0.25， &;=7.0.88Apache Tomcat &;=8.5.0，&;=8.5.31Apache Tomcat 9.09
CVSS分值	5.0
bugtraq编号	
CVE编号	CVE-2018-8034
CNCVE编号	CNCVE-20188034

国家漏洞库编号	CNNVD-201807-1992
CNVD编号	
简单描述	Apache Tomcat 安全漏洞(CVE-2018-8034)
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。Apache Tomcat 7.0.25版本至7.0.88版本、8.5.0版本至8.5.31版本和9.0.0.M1版本和9.0.9版本中存在安全绕过漏洞，该漏洞源于程序没有验证主机名称。远程攻击者可利用该漏洞绕过安全限制，执行未授权的操作。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接:http://tomcat.apache.org/security-7.htmlhttps://tomcat.apache.org/security-8.htmlhttp://tomcat.apache.org/security-9.html
参考网址	

【19】Apache Tomcat 安全绕过漏洞(CVE-2016-6796)	
漏洞编号	0x1ebc66
漏洞类型	WEB类
危险级别	中危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-2016-6796
CNCVE编号	CNCVE-20166796
国家漏洞库编号	CNNVD-201610-827
CNVD编号	0
简单描述	Apache Tomcat 安全绕过漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在安全管理绕过漏洞。攻击者可借助恶意的Web应用程序利用该漏洞绕过安全限制。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。

修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/5a2105a56b2495ab70fa568f06925bd861f0d71ffab4fb38bb4fdc45@%3Cannounce.tomcat.apache.org%3E
参考网址	链接:http://www.securityfocus.com/bid/93944

【20】Apache Tomcat 安全漏洞(CVE-2016-6794)	
漏洞编号	0x1ebc67
漏洞类型	WEB类
危险级别	中危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-2016-6794
CNCVE编号	CNCVE-20166794
国家漏洞库编号	CNNVD-201610-828
CNVD编号	0
简单描述	Apache Tomcat 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在安全漏洞。攻击者可利用该漏洞绕过安全限制。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://tomcat.apache.org/
参考网址	链接:http://www.securityfocus.com/bid/93943

【21】Apache Tomcat 安全绕过漏洞(CVE-2016-5018)	
漏洞编号	0x1ebc68
漏洞类型	WEB类
危险级别	中危险

影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-2016-5018
CNCVE编号	CNCVE-20165018
国家漏洞库编号	CNNVD-201610-829
CNVD编号	0
简单描述	Apache Tomcat 安全绕过漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在安全绕过漏洞。攻击者可借助恶意的Web应用程序利用该漏洞绕过安全限制。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://tomcat.apache.org/
参考网址	链接:http://www.securityfocus.com/bid/93942

【22】Apache Tomcat 信息泄露漏洞(CVE-2016-0762)	
漏洞编号	0x1ebc69
漏洞类型	WEB类
危险级别	中危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-2016-0762
CNCVE编号	CNCVE-20160762
国家漏洞库编号	CNNVD-201610-831
CNVD编号	0

简单描述	Apache Tomcat 信息泄露漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat中存在信息泄露漏洞。攻击者可利用该漏洞获取有效的用户名。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.apache.org/
参考网址	链接:http://www.securityfocus.com/bid/93939

【23】Apache Tomcat 安全漏洞(CVE-2016-6797)	
漏洞编号	0x1ebc6a
漏洞类型	WEB类
危险级别	中危险
影响平台	以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-2016-6797
CNCVE编号	CNCVE-20166797
国家漏洞库编号	CNNVD-201610-830
CNVD编号	0
简单描述	Apache Tomcat 安全漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat存在安全漏洞，该漏洞源于ResourceLinkFactory没有限制Web应用程序访问global JNDI资源。攻击者可利用该漏洞访问任意global JNDI资源。以下版本受到影响：Apache Tomcat 9.0.0.M1至9.0.0.M9版本，8.5.0至8.5.4版本，8.0.0.RC1至8.0.36版本，7.0.0至7.0.70版本，6.0.0至6.0.45版本。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://tomcat.apache.org/
参考网址	链接:http://www.securityfocus.com/bid/93940

【24】Apache Tomcat 信息泄露漏洞(CVE-2016-8745)	
漏洞编号	0x1ebc74
漏洞类型	WEB类
危险级别	中危险
影响平台	Apache Tomcat 9.0.0.M1至9.0.0.M13版本和8.5.0至8.5.8版本
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-2016-8745
CNCVE编号	CNCVE-20168745
国家漏洞库编号	CNNVD-201612-330
CNVD编号	0
简单描述	Apache Tomcat 信息泄露漏洞
详细描述	Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。;Apache Tomcat 9.0.0.M1至9.0.0.M13版本和8.5.0至8.5.8版本中存在信息泄露漏洞。攻击者可利用该漏洞获取敏感信息。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：http://tomcat.apache.org/security-8.htmlhttp://tomcat.apache.org/security-9.html
参考网址	链接:http://www.securityfocus.com/bid/94828

【25】Apache Tomcat CORS Filter 安全漏洞(CVE-2017-7674)	
漏洞编号	0xb2d36fe7
漏洞类型	Apache类
危险级别	中危险
影响平台	9.0.0.M1版本至9.0.0.M21版本，8.5.0版本至8.5.15版本，8.0.0.RC1版本至8.0.44版本，7.0.41版本至7.0.78版本。
CVSS分值	4.3
bugtraq编号	
CVE编号	CVE-2017-7674

CNCVE编号	CNCVE-20177674
国家漏洞库编号	CNNVD-201704-577
CNVD编号	
简单描述	Apache Tomcat CORS Filter 安全漏洞,Apache Tomcat是美国阿帕奇（Apache）软件基金会下属的Jakarta项目的一款轻量级Web应用服务器，它主要用于开发和调试JSP程序，适用于中小型系统。CORS Filter是其中的一个提供跨源资源共享功能的组件。
详细描述	Apache Tomcat中的CORS Filter存在安全漏洞，该漏洞源于程序没有添加特定的HTTP Vary包头。攻击者可利用该漏洞造成客户端和服务器端缓存中毒。以下版本受到影响：Apache Tomcat 9.0.0.M1版本至9.0.0.M21版本，8.5.0版本至8.5.15版本，8.0.0.RC1版本至8.0.44版本，7.0.41版本至7.0.78版本。
修补建议	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/22b4bb077502f847e2b9fcf00b96e81e734466ab459780ff73b60c0f@%3Cannounce.tomcat.apache.org%3E
参考网址	

【26】远程主机DISCARD服务正在运行	
漏洞编号	00300AB
漏洞类型	信息收集类
危险级别	低危险
影响平台	DISCARD
CVSS分值	2.1
bugtraq编号	
CVE编号	CVE-1999-0636
CNCVE编号	CNCVE-19990636
国家漏洞库编号	
CNVD编号	
简单描述	远程主机DISCARD服务正在运行
详细描述	远程主机DISCARD服务正在运行
修补建议	建议您采取以下措施进行修补以降低威胁： 若不需要，禁止该服务。

参考网址	

【27】检测到目标主机IIS服务正在运行	
漏洞编号	0x0013026A
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	IIS 是一个WWW服务
详细描述	IIS是一种Web（网页）服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面
修补建议	信息收集，无需修复
参考网址	

【28】检测到远程主机HTTP Server正在运行	
漏洞编号	0x001303CC
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	

国家漏洞库编号	
CNVD编号	
简单描述	一个开放源代码的网页服务器
详细描述	可以在大多数电脑操作系统中运行，由于其具有的跨平台性和安全性，被广泛使用，是最流行的Web服务器端软件之一。
修补建议	信息收集，无需修复
参考网址	

【29】可通过NetBIOS名字服务端口远程获取系统信息	
漏洞编号	0x001303E2
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	NETBIOS协议是由IBM公司开发，主要用于数十台计算机的小型局域网。
详细描述	该协议是一种在局域网上的程序可以使用的应用程序编程接口（API），为程序提供了请求低级服务的统一的命令集，作用是为了给局域网提供网络以及其他特殊功能。
修补建议	信息收集，无需修复
参考网址	

【30】检测到目标主机Apache Tomcat正在运行	
漏洞编号	0x0013048C
漏洞类型	信息收集类

危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	Apache是普通服务器，本身只支持html即普通网页。不过可以通过插件支持php还可以与Tomcat连通单向Apache连接Tomcat就是说通过Apache可以访问Tomcat资源。反之不然。
详细描述	Apache Tomcat 包含了一个配置管理工具，也可以通过编辑 XML 格式的配置文件来进行配置。Apache，nginx，tomcat并称为网页服务三剑客，可见其应用度之广泛。
修补建议	信息收集，无需修复
参考网址	

【31】ICMP权限许可和访问控制漏洞CVE-1999-0524	
漏洞编号	001E93A6
漏洞类型	CGI类
危险级别	信息
影响平台	所有系统
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-1999-0524
CNCVE编号	CNCVE-19990524
国家漏洞库编号	0!#!
CNVD编号	
简单描述	ICMP权限许可和访问控制漏洞
详细描述	ICMP信息如netmask和timestamp允许任意主机访问。

修补建议	配置防火墙或过滤路由器以阻止传出的ICMP数据包。阻止类型13或14和/或代码0的ICMP数据包
参考网址	

【32】回声服务运行漏洞CVE-1999-0635	
漏洞编号	001E97EB
漏洞类型	CGI类
危险级别	信息
影响平台	echo
CVSS分值	0.0
bugtraq编号	
CVE编号	CVE-1999-0635
CNCVE编号	CNCVE-19990635
国家漏洞库编号	0!#!
CNVD编号	
简单描述	回声服务运行漏洞
详细描述	回声服务正在运行。
修补建议	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接:http://secunia.com/advisories/18514
参考网址	URL:http://secunia.com/advisories/18514

【33】目标主机允许Traceroute探测	
漏洞编号	0x1ebc5e
漏洞类型	信息收集类
危险级别	信息
影响平台	Traceroute
CVSS分值	0.0
bugtraq编号	

CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	0
简单描述	目标主机允许Traceroute探测
详细描述	使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者可以利用这些信息来了解目标网络的网络拓扑。
修补建议	信息收集，无需修复
参考网址	

【34】远程主机HTTP协议版本信息泄漏	
漏洞编号	0x1ebe9a
漏洞类型	WEB类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	远程获取主机的HTTP协议版本信息
详细描述	远程获取主机的HTTP协议版本信息，这些信息可能会帮助攻击者决定如何对目标靶机进行攻击。
修补建议	可以修改WEB服务器配置，隐藏协议版本信息。
参考网址	

【35】目标主机运行着ECHO服务

漏洞编号	0xb2d36c71
漏洞类型	信息收集类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
简单描述	ECHO服务是一种互联网协议,由RFC 862定义。
详细描述	ECHO服务是一种互联网协议,由RFC 862定义。可以通过发送echo包知道当前的连接节点有那些路径，并且通过往返时间能得出路径长度
修补建议	如果没有必要，关闭此服务
参考网址	

【36】通过HTTP获取目标主机的WWW服务信息	
漏洞编号	0xb2d36ca2
漏洞类型	WEB类
危险级别	信息
影响平台	
CVSS分值	0.0
bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	

简单描述	探测到目标主机的HTTP Server信息。这可能使得攻击者了解远程www服务的类型，以便进行下一步的攻击。
详细描述	探测到目标主机的HTTP Server信息。这可能使得攻击者了解远程www服务的类型，以便进行下一步的攻击。
修补建议	建议隐藏您HTTP服务器的banner信息
参考网址	