安全报告

天镜

脆弱性扫描与管理系统

Cybervision Vulnerability
Assessment and management System

报表名称：report_.国发污染源监控平台_20190703
单位名称：安徽省生态环境厅
提 交 人：配置管理员
生成日期：2019-07-03

北京启明星辰信息安全技术有限公司
Beijing Venustech Security Inc.

1章节目录

章节目录

2 任务概述

2.1 任务信息

任务名称	国发污染源监控平台
任务类型	漏洞扫描任务
创建者	配置管理员
开始时间	2019-07-03 16:00:38
任务耗时	5分57秒
任务状态	已完成
执行方式	立即执行
在线主机数	5
扫描策略	常规安全扫描
扫描目标	10.34.100.150 10.34.100.35 10.34.100.107 10.34.100.151 10.34.100.159
排除目标	--

2.2 高级参数

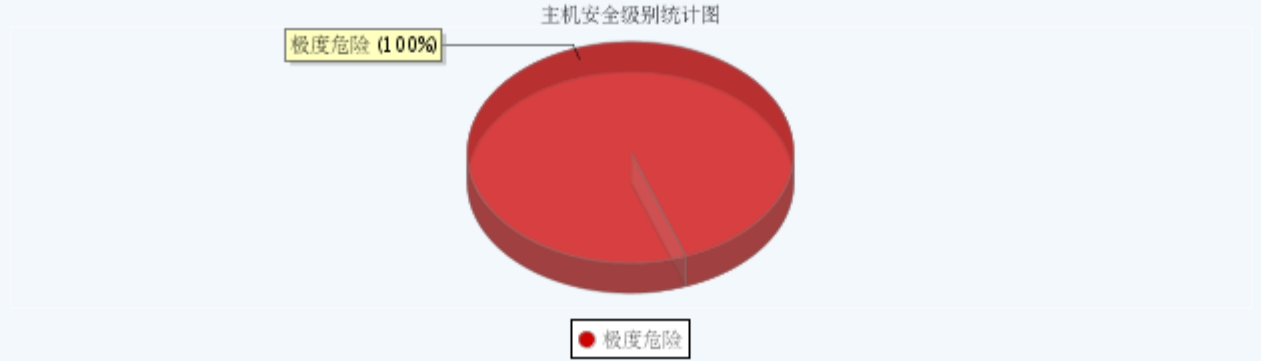
主机存活探测类型	常规探测
自定义主机存活探测端口	--
是否开启端口扫描策略	是
端口扫描策略	标准端口扫描
是否指定端口扫描	否
指定扫描端口	--
端口扫描方式	SYN|ACK
开启UDP扫描	否
使用智能服务识别	否
任务优先级	低

插件超时时间(秒)	40
是否断网续扫	否
最大并行扫描主机数	20
每个主机最大线程数	--
扫描项间隔时间(毫秒)	0
是否按操作系统扫描	是
是否通知被扫描主机	否
通知内容	--
是否执行Windows域扫描	否
发送延迟(秒)	1
接收延迟(秒)	2
连接延迟(秒)	2
是否启用口令猜测	否
口令猜测时间(分)	20
是否启用授权方式检测	否
是否启用旧有口令扫描方式检测	否

3 统计信息

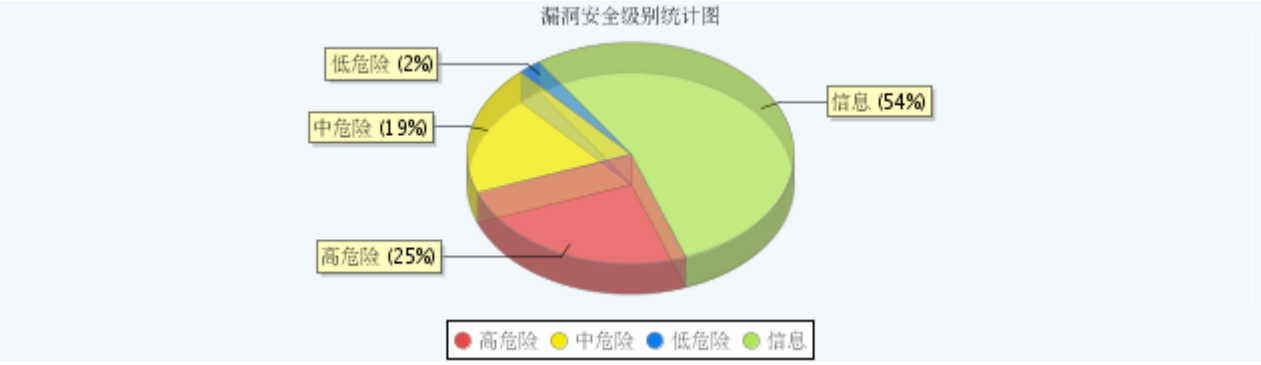
3.1 主机风险分布

安全级别	主机数量	百分比
极度危险	5	100%
		主机数总计:5



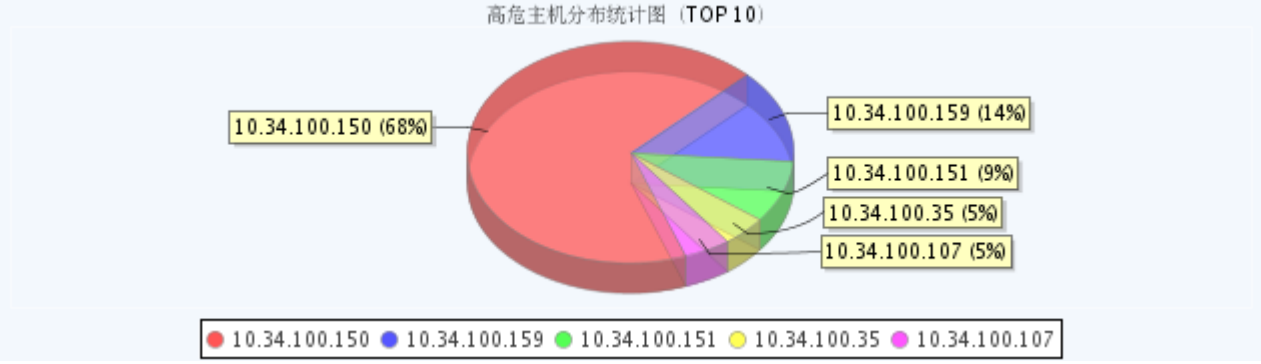
3.2 漏洞风险分布

危险级别	漏洞数量	百分比
高危险	22	25%
中危险	17	19%
低危险	2	2%
信息	48	54%
		漏洞数量合计:89



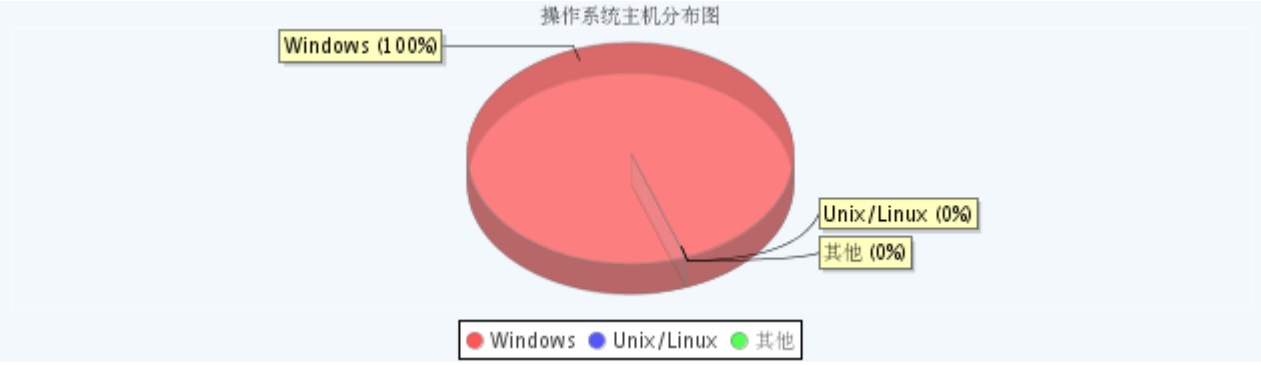
3.3 高危漏洞的主机分布

序号	主机IP	高危漏洞数量	百分比
1	10.34.100.150	15	68%
2	10.34.100.159	3	14%
3	10.34.100.151	2	9%
4	10.34.100.35	1	5%
5	10.34.100.107	1	5%
漏洞数量合计:22			



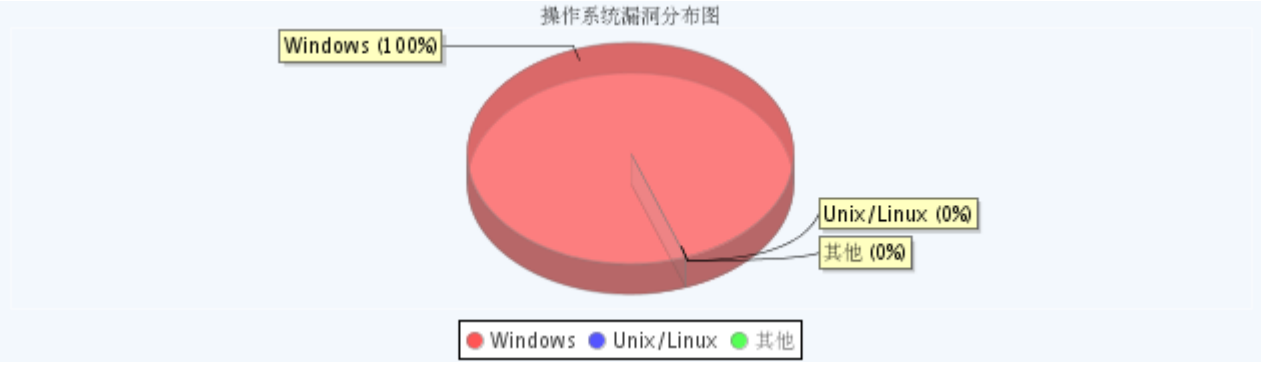
3.4 操作系统主机分布

序号	操作系统信息	极度危险主机数	高度危险主机数	中度危险主机数	低度危险主机数	比较安全主机数	主机数量
1	Windows	5	0	0	0	0	5
2	Unix/Linux	0	0	0	0	0	0
3	其他	0	0	0	0	0	0



3.5 操作系统漏洞分布

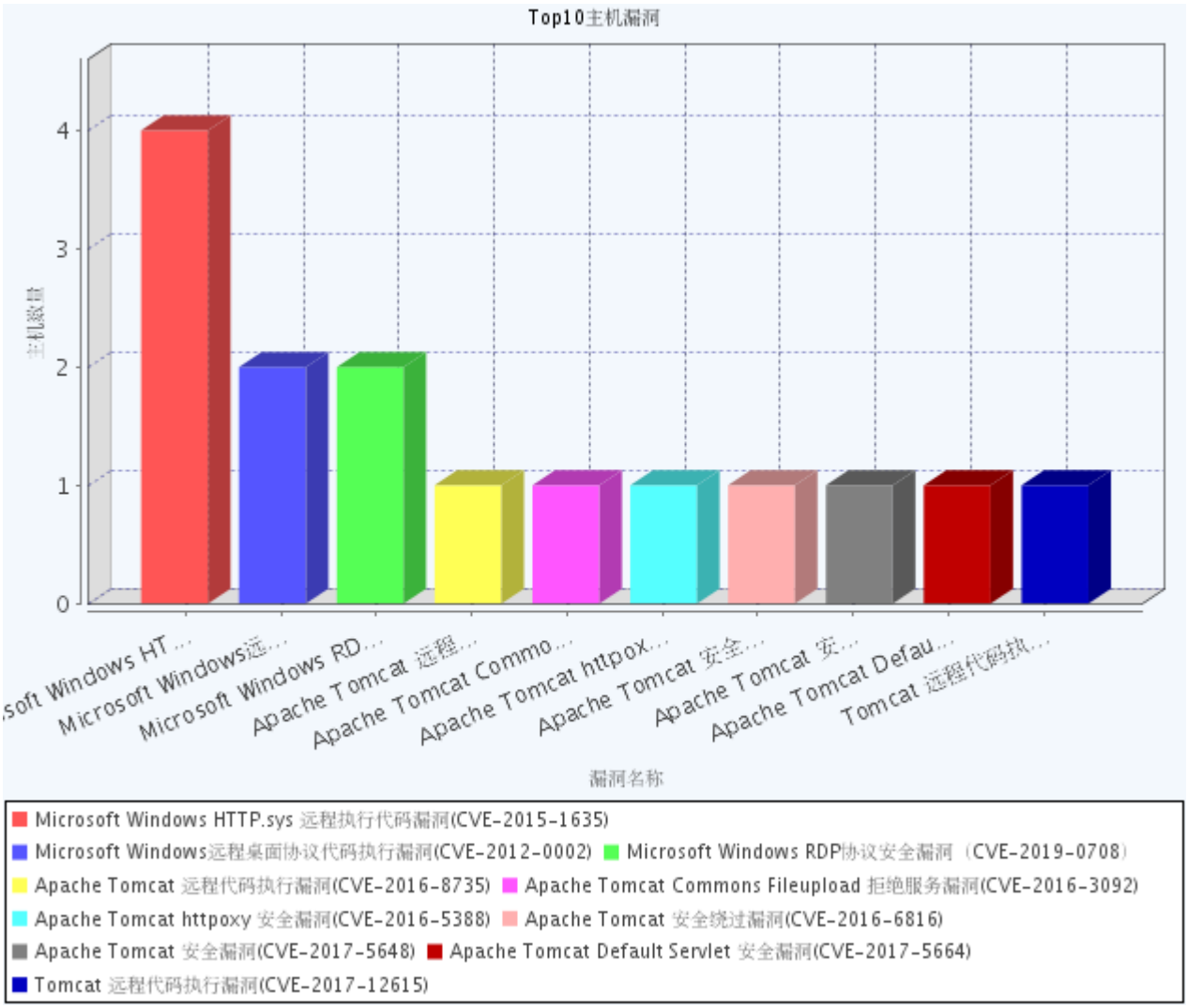
序号	操作系统信息	高危漏洞数	中危漏洞数	低危漏洞数	信息类漏洞数	漏洞数量合计
1	Windows	22	17	2	48	89
2	Unix/Linux	0	0	0	0	0
3	其他	0	0	0	0	0



3.6 Top10高危漏洞

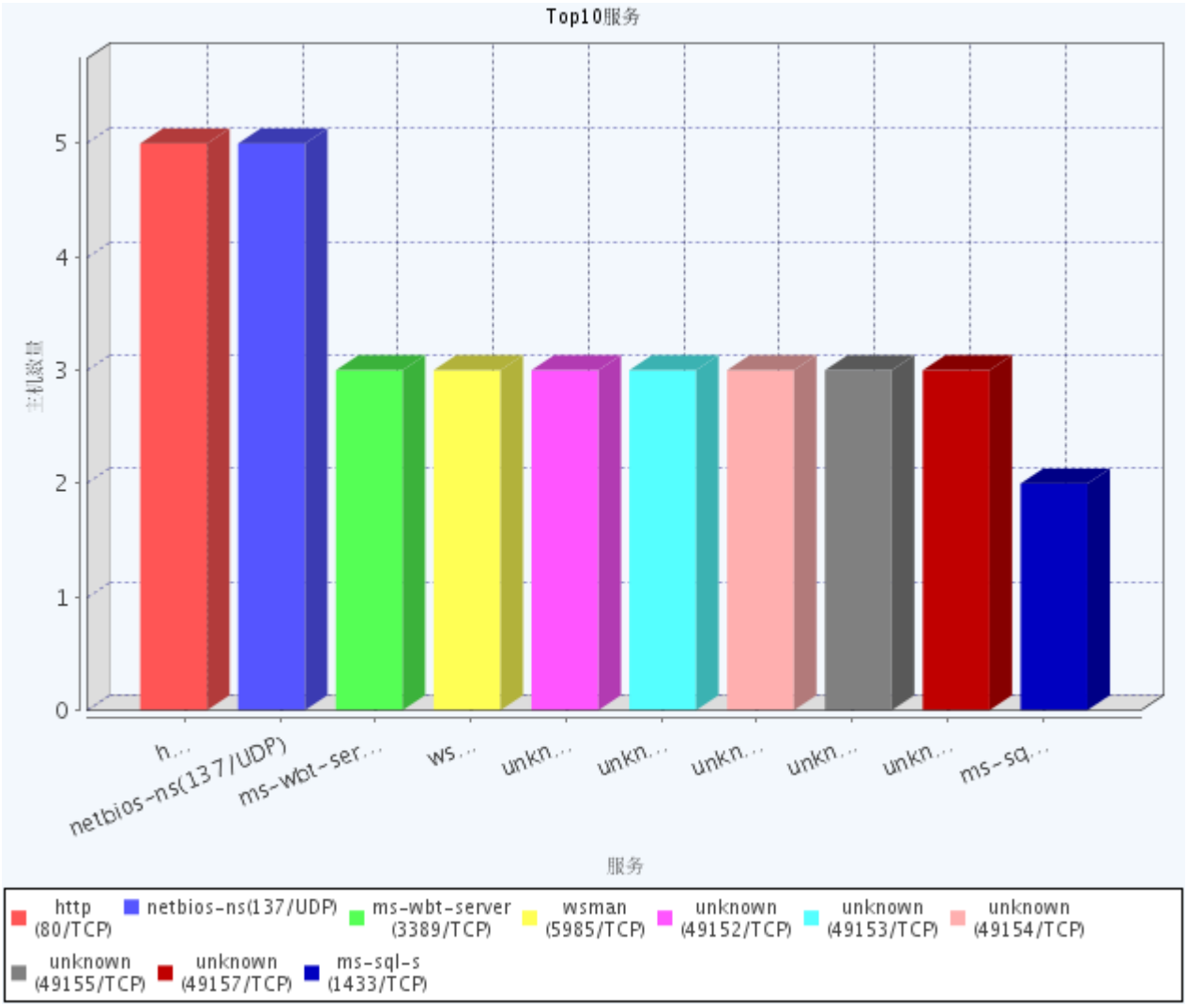
序号	漏洞名称	危险级别	主机数量	漏洞类型	CVE编号	存在主机
1	Microsoft Windows HTTP.sys 远程执行代码漏洞(CVE-2015-1635)	高危险	4	NT关键问题类	CVE-2015-1635	10.34.100.107 10.34.100.159 10.34.100.35 10.34.100.150
2	Microsoft Windows远程桌面协议代码执行漏洞(CVE-2012-0002)	高危险	2	NT关键问题类	CVE-2012-0002	10.34.100.151 10.34.100.159
3	Microsoft Windows RDP协议安全漏洞（CVE-2019-0708）	高危险	2	NT补丁类	CVE-2019-0708	10.34.100.151 10.34.100.159
4	Apache Tomcat 远程代码执行漏洞(CVE-2016-8735)	高危险	1	WEB类	CVE-2016-8735	10.34.100.150
5	Apache Tomcat Commons Fileupload 拒绝服务漏洞(CVE-2016-3092)	高危险	1	Apache类	CVE-2016-3092	10.34.100.150

6	Apache Tomcat httpoxy 安全漏洞(CVE-2016-5388)	高危险	1	WEB类	CVE-2016-5388	10.34.100.150
7	Apache Tomcat 安全绕过漏洞(CVE-2016-6816)	高危险	1	WEB类	CVE-2016-6816	10.34.100.150
8	Apache Tomcat 安全漏洞(CVE-2017-5648)	高危险	1	WEB类	CVE-2017-5648	10.34.100.150
9	Apache Tomcat Default Servlet 安全漏洞(CVE-2017-5664)	高危险	1	WEB类	CVE-2017-5664	10.34.100.150
10	Tomcat 远程代码执行漏洞(CVE-2017-12615)	高危险	1	WEB类	CVE-2017-12615	10.34.100.150



3.7 Top10服务

序号	端口	协议	服务	描述	主机数量	存在主机
1	80	TCP	http	WWW services support TRACE requests	5	10.34.100.150 10.34.100.107 10.34.100.159 10.34.100.35 10.34.100.151
2	137	UDP	netbios-ns	--	5	10.34.100.151 10.34.100.150 10.34.100.107 10.34.100.159 10.34.100.35
3	3389	TCP	ms-wbt-server	--	3	10.34.100.159 10.34.100.35 10.34.100.151
4	5985	TCP	wsman	--	3	10.34.100.107 10.34.100.150 10.34.100.35
5	49152	TCP	unknown	--	3	10.34.100.107 10.34.100.35 10.34.100.150
6	49153	TCP	unknown	--	3	10.34.100.35 10.34.100.150 10.34.100.107
7	49154	TCP	unknown	--	3	10.34.100.107 10.34.100.35 10.34.100.150
8	49155	TCP	unknown	--	3	10.34.100.150 10.34.100.107 10.34.100.35
9	49157	TCP	unknown	--	3	10.34.100.35 10.34.100.150 10.34.100.107
10	1433	TCP	ms-sql-s	Detected Microsoft SQL Server Version: 10.50.1600.0 Location: 1433/tcp CPE: cpe:/a:microsoft:sql_server:10.50.1600.0 Concluded from version/product identification result: Remote probe	2	10.34.100.159 10.34.100.107


Top10服务
主机数量
0
1
2
3
4
5
h...
netbios-ns(137/UDP)
ms-wbt-ser...
ws...
unkn...
unkn...
unkn...
unkn...
unkn...
ms-sq...
服务
http (80/TCP)
netbios-ns(137/UDP)
ms-wbt-server (3389/TCP)
wsman (5985/TCP)
unknown (49152/TCP)
unknown (49153/TCP)
unknown (49154/TCP)
unknown (49155/TCP)
unknown (49157/TCP)
ms-sql-s (1433/TCP)

4 账号分布

4.1 账号分布

主机IP	猜测类型	用户名	密码(隐藏)	描述
N/A				

注：基于保密原因，密码进行密文显示

5 主机详细

5.1 主机扫描统计列表

注：主机详细的具体内容，请参看离线报表文件

序号	主机IP	漏洞数量合计	高危漏洞数	中危漏洞数	低危漏洞数	信息类漏洞数	服务总数	用户总数	风险分值	安全状态
1	10.34.100.35	19	1	3	1	14	23	0	844.80	极度危险
2	10.34.100.107	12	1	2	0	9	13	0	849.14	极度危险
3	10.34.100.150	36	15	10	1	10	26	0	1023.82	极度危险
4	10.34.100.151	10	2	2	0	6	4	0	930.05	极度危险
5	10.34.100.159	12	3	0	0	9	11	0	1003.70	极度危险

6 漏洞详细

6.1 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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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/
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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

漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【13】Microsoft Windows远程桌面协议代码执行漏洞(CVE-2012-0002)【原理扫描】	
漏洞编号	0xb2d3957fL
漏洞类型	NT关键问题类
危险级别	高危险

影响平台	该漏洞已有修复补丁，如果未能及时安装补丁可采取以下临时修复措施：方法一：禁用终端服务、远程桌面、远程协助和 Windows Small Business Server 2003 远程工作网站功能；方法二：在企业周边防火墙中屏蔽TCP端口3389；方法三：在运行 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 的受支持版本
CVSS分值	9.3
bugtraq编号	
CVE编号	CVE-2012-0002
CNCVE编号	CNCVE-20120002
国家漏洞库编号	CNNVD-201203-241
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.151　10.34.100.159
简单描述	Microsoft Windows是美国微软（Microsoft）公司发布的一系列操作系统
详细描述	Microsoft Windows是美国微软（Microsoft）公司发布的一系列操作系统。Microsoft Windows XP SP2与SP3， Windows Server 2003 SP2， Windows Vista SP2， Windows Server 2008 SP2， R2及R2 SP1，与Windows 7 Gold与SP1版本中的远程桌面协议(RDP)实现中存在漏洞，该漏洞源于没有正确处理内存中的数据包。远程攻击者可通过发送特制RDP数据包触发访问（1）没有正确初始化或者（2）已被删除的对象，执行任意代码。也称‘ Remote Desktop Protocol Vulnerability ’。该漏洞已有修复补丁，如果未能及时安装补丁可采取以下临时修复措施：方法一：禁用终端服务、远程桌面、远程协助和 Windows Small Business Server 2003 远程工作网站功能；方法二：在企业周边防火墙中屏蔽TCP端口3389；方法三：在运行 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 的受支持版本的系统上启用网络级别身份验证。
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://technet.microsoft.com/zh-cn/security/bulletin/ms12-020
参考网址	URL:http://www.nsfocus.net/vulndb/19054,Source:NSFOCUS;URL:http://www.nsfocus.net/vulndb/19054http://secunia.com/advisories/48353,Source:SECUNIA;URL:http://www.nsfocus.net/vulndb/19054http://secunia.com/advisories/48353http://technet.microsoft.com/security/bulletin/MS12-020,Source:MS;
漏洞安全性	

【14】Apache Tomcat CORS Filter 安全漏洞(CVE-2018-8014)	
漏洞编号	0xb2d3bf65
漏洞类型	Apache类

漏洞详细

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	
漏洞可利用性	
存在主机	10.34.100.150
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;
漏洞安全性	

【15】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【16】Microsoft Windows RDP协议安全漏洞（CVE-2019-0708）【原理扫描】	
漏洞编号	0xb2d3c1ca
漏洞类型	NT补丁类
危险级别	高危险
影响平台	Windows 7, Windows 2008 R2, and Windows 2008， Windows 2003 and Windows XP
CVSS分值	10.0
bugtraq编号	
CVE编号	CVE-2019-0708

CNCVE编号	CNCVE-20190708
国家漏洞库编号	CNNVD-201905-434
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.151　10.34.100.159
简单描述	通过Remote Desktop Service（远程桌面服务）向目标设备发送特制的请求，可以在不需要用户干预的情况下远程执行任意代码
详细描述	通过Remote Desktop Service（远程桌面服务）向目标设备发送特制的请求，可以在不需要用户干预的情况下远程执行任意代码，最终可能会像野火一样蔓延至整个系统，从而让整个系统瘫痪
修补建议	厂商已经发布补丁，获取地址https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/?from=groupmessage&isappinstalled=0
参考网址	
漏洞安全性	

【17】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	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.107　10.34.100.150　10.34.100.159

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
漏洞安全性	

【18】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【19】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【20】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【21】Microsoft SQL Server 堆栈溢出漏洞(CVE-2014-4061)	
漏洞编号	00200B2
漏洞类型	NT应用程序类
危险级别	中危险
影响平台	Microsoft SQL Server 2008 SP3 2008 R2 SP2 and 2012 SP1
CVSS分值	6.8
bugtraq编号	

CVE编号	CVE-2014-4061
CNCVE编号	CNCVE-20144061
国家漏洞库编号	CNNVD-201408-210
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.107
简单描述	Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统
详细描述	Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统。 Microsoft SQL Server中存在一个拒绝服务漏洞。成功利用此漏洞的攻击者可造成拒绝服务，导致服务器停止响应。以下软件受到影响：Microsoft SQL Server 2008 SP3，2008 R2 SP2，2012 SP1。
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/ms14-044
参考网址	CONFIRM:http://blogs.technet.com/b/srd/archive/2014/08/12/assessing-risk-for-the-august-2014-security-updates.aspx MS:MS14-044 URL:http://technet.microsoft.com/security/bulletin/MS14-044
漏洞安全性	

【22】Microsoft SQL Master Data Services XSS 漏洞(CVE-2014-1820)	
漏洞编号	00200B3
漏洞类型	NT应用程序类
危险级别	中危险
影响平台	Microsoft SQL Server 2012 SP1 and 2014 on 64-bit platforms
CVSS分值	4.3
bugtraq编号	
CVE编号	CVE-2014-1820
CNCVE编号	CNCVE-20141820
国家漏洞库编号	CNNVD-201408-182

CNVD编号	
漏洞可利用性	
存在主机	10.34.100.107
简单描述	Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统
详细描述	Microsoft SQL Server是美国微软（Microsoft）公司开发和维护的一套应用在Microsoft Windows系统下的大型商业数据库系统。Master Data Services（MDS）是其中的一个主数据服务。 用于x64位系统Microsoft SQL Server 2012 SP1和2014版本的SQL MDS中存在XSS漏洞，该漏洞可能允许攻击者在用户的Internet Explorer实例中注入客户端脚本。该脚本可能欺骗内容、泄露信息或执行用户可以在网站上代表目标用户执行的任何操作。
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/ms14-044
参考网址	MS:MS14-044 URL:http://technet.microsoft.com/security/bulletin/MS14-044
漏洞安全性	

【23】RC4 加密问题漏洞CVE-2015-2808【原理扫描】	
漏洞编号	001E88F7
漏洞类型	其他漏洞
危险级别	中危险
影响平台	Microsoft IIS nullMozilla Firefox nullOpera Opera Browser nullApple Safari Google Chrome IBM WebSphere Application Server RedHat JBoss Oracle Glassfish Microsoft IE
CVSS分值	4.3
bugtraq编号	
CVE编号	CVE-2015-2808
CNCVE编号	CNCVE-20152808
国家漏洞库编号	0!#!
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.151
简单描述	RC4 加密问题漏洞

详细描述	TLS协议和SSL协议中使用的RC4算法中存在安全漏洞，该漏洞源于程序在初始化阶段没有正确组合状态数据和密钥数据。远程攻击者可通过嗅探特定的网络流量，然后实施暴力破解攻击利用该漏洞对数据流中的初始化字节实施plaintext-recovery攻击。
修补建议	禁用RC4算法。请参考https://blog.csdn.net/Nedved_L/article/details/81110603以及https://support.microsoft.com/zh-cn/help/2868725/microsoft-security-advisory-update-for-disabling-rc4
参考网址	CONFIRM:http://www-01.ibm.com/support/docview.wss?uid=swg21883640
漏洞安全性	

【24】TLS/SSL协议 RC4算法安全漏洞CVE-2013-2566【原理扫描】	
漏洞编号	001EA184
漏洞类型	CGI类
危险级别	中危险
影响平台	
CVSS分值	5.9
bugtraq编号	
CVE编号	CVE-2013-2566
CNCVE编号	CNCVE-20132566
国家漏洞库编号	0!#!
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.151
简单描述	TLS/SSL协议 RC4算法安全漏洞
详细描述	TLS协议和SSL协议中使用的的RC4算法中存在漏洞，该漏洞源于使用大量的单字节偏差。通过在使用相同明文的大量会话中密文的统计分析，远程攻击者利用该漏洞进行明文恢复攻击。
修补建议	禁用RC4算法。请参考https://blog.csdn.net/Nedved_L/article/details/81110603以及https://support.microsoft.com/zh-cn/help/2868725/microsoft-security-advisory-update-for-disabling-rc4
参考网址	MISC:http://cr.yp.to/talks/2013.03.12/slides.pdf
漏洞安全性	

【25】DES和Triple DES 信息泄露漏洞(CVE-2016-2183)【原理扫描】	
漏洞编号	0x1eb685
漏洞类型	信息收集类
危险级别	中危险
影响平台	in the TLS SSH and IPSec protocols and other protocols and products have a birthday bound of approximately four billion blocks makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session
CVSS分值	5.3
bugtraq编号	
CVE编号	CVE-2016-2183
CNCVE编号	CNCVE-20162183
国家漏洞库编号	CNNVD-201608-448
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	DES和Triple DES 信息泄露漏洞
详细描述	TLS（Transport Layer Security，安全传输层协议）是一套用于在两个通信应用程序之间提供保密性和数据完整性的协议。SSH（全称Secure Shell）是国际互联网工程任务组（IETF）的网络小组（Network Working Group）所制定的一套创建在应用层和传输层基础上的安全协议。IPSec（全称InternetProtocolSecurity）是国际互联网工程任务组（IETF）的IPSec小组建立的一组IP安全协议集。DES和Triple DES都是加密算法。;TLS、SSH和IPSec协议和其它协议及产品中使用的DES和Triple DES密码算法存在安全漏洞。远程攻击者可通过实施生日攻击利用该漏洞获取明文数据。
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.openssl.org/blog/blog/2016/08/24/sweet32/

参考网址	链接:https://sweet32.info/ 链接:https://www.sigsac.org/ccs/CCS2016/accepted-papers/ 链接:https://github.com/ssllabs/ssllabs-scan/issues/387#issuecomment-242514633 链接:https://www.openssl.org/blog/blog/2016/08/24/sweet32/ 链接:https://access.redhat.com/security/cve/cve-2016-2183 链接:https://nakedsecurity.sophos.com/2016/08/25/anatomy-of-a-cryptographic-collision-the-sweet32-attack/ 链接:https://www.teskalabs.com/blog/teskalabs-bulletin-160826-seacat-sweet32-issue 链接:https://www.ietf.org/mail-archive/web/tls/current/msg04560.html 链接:https://blog.cryptographyengineering.com/2016/08/24/attack-of-week-64-bit-ciphers-in-tls/ 链接:https://access.redhat.com/articles/2548661 链接:https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2016/august/new-practical-attacks-on-64-bit-block-ciphers-3des-blowfish/ 链接:https://bugzilla.redhat.com/show_bug.cgi?id=1369383 链接:http://www.securityfocus.com/bid/92630
漏洞安全性	

【26】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【27】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【28】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【29】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【30】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【31】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【32】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【33】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【34】SSL3.0 加密协议信息泄露漏洞(CVE-2014-3566)【原理扫描】	
漏洞编号	004119A
漏洞类型	WEB类
危险级别	低危险
影响平台	OpenSSL through 1.0.1i

漏洞详细

CVSS分值	3.1
bugtraq编号	
CVE编号	CVE-2014-3566
CNCVE编号	CNCVE-20143566
国家漏洞库编号	CNNVD-201410-267
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	SSL protocol是Secure Socket Layer（安全套接层协议）的缩写，其目的是为互联网通信提供安全及数据完整性保障。
详细描述	SSL protocol是Secure Socket Layer（安全套接层协议）的缩写，其目的是为互联网通信提供安全及数据完整性保障。OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 1.0.1i及之前版本中使用的SSL protocol 3.0版本中存在安全漏洞，该漏洞源于程序使用非确定性的CBC填充。攻击者可借助padding-oracle攻击利用该漏洞实施中间人攻击，获取明文数据。
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.openssl.org/news/
参考网址	MLIST:[openssl-dev] 20141014 Patch to mitigate CVE-2014-3566 ("POODLE") URL:http://marc.info/?l=openssl-dev&m=141333049205629&w=2 MISC:http://googleonlinesecurity.blogspot.com/2014/10/this-poodle-bites-exploiting-ssl-30.html MISC:https://www.openssl.org/~bodo/ssl-poodle.pdf MISC:http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-2014-3566 MISC:http://blog.cryptographyengineering.com/2014/10/attack-of-week-poodle.html MISC:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html MISC:https://www.imperialviolet.org/2014/10/14/poodle.html CONFIRM:http://blogs.technet.com/b/msrc/archive/2014/10/14/security-advisory-3009008-released.aspx CONFIRM:https://technet.microsoft.com/library/security/3009008.aspx CONFIRM:http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-3566.html CONFIRM:https://access.redhat.com/articles/1232123 CONFIRM:https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/ CONFIRM:https://bugzilla.mozilla.org/show_bug.cgi?id=1076983 CONFIRM:https://bugzilla.redhat.com/show_bug.cgi?id=1152789 CONFIRM:https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip CONFIRM:https://www.suse.com/support/kb/doc.php?id=7015773

漏洞安全性	

【35】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	
漏洞可利用性	
存在主机	10.34.100.35 10.34.100.107 10.34.100.150 10.34.100.151 10.34.100.159
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	
漏洞安全性	

【36】检测到远程主机运行着Microsoft SQL Server	
漏洞编号	0x001303C8
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	
漏洞可利用性	
存在主机	10.34.100.107　10.34.100.159
简单描述	SQL Server 是Microsoft 公司推出的关系型数据库管理系统。
详细描述	Microsoft SQL Server 是一个全面的数据库平台，使用集成的商业智能 BI工具提供了企业级的数据管理。Microsoft SQL Server 数据库引擎为关系型数据和结构化数据提供了更安全可靠的存储功能，使您可以构建和管理用于业务的高可用和高性能的数据应用程序。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【37】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	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.107　10.34.100.150　10.34.100.151　10.34.100.159

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	
漏洞安全性	

【38】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	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.107　10.34.100.150　10.34.100.151　10.34.100.159
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	
漏洞安全性	

【39】检测到远程主机FileMaker service服务正在运行	
漏洞编号	0x00130403

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	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	FileMaker是一款功能强大且简单易用的数据库软件
详细描述	用于创建可在 iPad、iPhone、Windows、Mac 和 Web 上运行的自定义商业解决方案。可使用 FileMaker Pro 管理信息，并与团队共享信息。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【40】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【41】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	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.107　10.34.100.150　10.34.100.159
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	

漏洞安全性	

【42】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	
漏洞可利用性	
存在主机	10.34.100.150
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
漏洞安全性	

【43】远程服务使用的是自签名的证书	
漏洞编号	0x1ebc5d
漏洞类型	OpenSSL
危险级别	信息
影响平台	SSL
CVSS分值	0.0

bugtraq编号	
CVE编号	
CNCVE编号	
国家漏洞库编号	
CNVD编号	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	远程服务使用的是自签名的证书
详细描述	目标机器提供的服务使用的是自签名的证书，请确保您的通信安全。
修补建议	请检查证书，及时更换认证证书。
参考网址	
漏洞安全性	

【44】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	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.107　10.34.100.150　10.34.100.151　10.34.100.159
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	
漏洞安全性	

【45】目标服务加密通信使用的SSL加密算法可列取	
漏洞编号	0x1ebda1
漏洞类型	OpenSSL
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	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	目标服务加密通信使用的SSL加密算法可获取。
详细描述	SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【46】SSL弱加密算法检查【原理扫描】	
漏洞编号	0x1ebda2

漏洞类型	OpenSSL
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	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	目标机器存在SSL弱加密算法
详细描述	SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【47】SSL证书使用了弱签名算法sha1【原理扫描】	
漏洞编号	0x1ebe19
漏洞类型	其他漏洞
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	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	SSL证书使用了弱签名算法sha1
详细描述	SSL证书使用了弱签名算法sha1
修补建议	可通过配置禁用弱签名算法.
参考网址	
漏洞安全性	

【48】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	
漏洞可利用性	
存在主机	10.34.100.35 10.34.100.107 10.34.100.150 10.34.100.151 10.34.100.159
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	

漏洞安全性	

【49】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	
漏洞可利用性	
存在主机	10.34.100.150
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	
漏洞安全性	

【50】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	
漏洞可利用性	
存在主机	10.34.100.35　10.34.100.107　10.34.100.150　10.34.100.151　10.34.100.159
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	
漏洞安全性	

【51】可获取目标服务支持的SSL加密协议	
漏洞编号	0xb2d37168
漏洞类型	DNS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	
漏洞可利用性	
存在主机	10.34.100.35

简单描述	可获取目标服务支持的SSL加密协议
详细描述	SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在传输层对网络连接进行加密。
修补建议	扫描过程中获取的信息，可以不做修复。
参考网址	
漏洞安全性	

【52】远程探测到Microsoft SQL Server正在运行	
漏洞编号	0xb2d3b153
漏洞类型	MSSQL系统配置
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	
漏洞可利用性	
存在主机	10.34.100.107　10.34.100.159
简单描述	Microsoft SQL Server是一款流行的SQL数据库系统
详细描述	Microsoft SQL Server是一款流行的SQL数据库系统
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

【53】探测到Hyper-V管理服务正在运行	
漏洞编号	0xb2d3c186

漏洞详细

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	
漏洞可利用性	
存在主机	10.34.100.35
简单描述	探测到Hyper-V管理服务正在运行
详细描述	Hyper-V是微软提出的一种系统管理程序虚拟化技术，能够实现桌面虚拟化
修补建议	信息收集，无需修复
参考网址	
漏洞安全性	

7 参考信息

7.1 主机安全等级标准

安全级别	风险值区域
极度危险	256<=主机风险值<=1024
高度危险	64<=主机风险值<256
中度危险	16<=主机风险值<64
低度危险	4<=主机风险值<16
比较安全	0<=主机风险值<4

7.2 网络安全等级标准

安全级别	风险值区域
极度危险	256<=网络风险值<=1024
高度危险	64<=网络风险值<256
中度危险	16<=网络风险值<64
低度危险	4<=网络风险值<16
比较安全	0<=网络风险值<4

7.3 漏洞危险等级标准

危险级别	风险值区域
高危险	7<=漏洞风险值<=10
中危险	4<=漏洞风险值<=7
低危险	1<=漏洞风险值<=4
信息	0<=漏洞风险值<=1

8 安全结论

8.1 安全结论

一、任务概述
2019-07-03,对国发污染源监控平台任务进行了漏洞扫描,采用常规安全扫描策略。共发现存活主机5台,漏洞89个,网络安全状态等级为极度危险。
其中发现比较安全主机0台,低度危险主机0台,中度危险主机0台,高度危险主机0台,极度危险主机5台,
信息类漏洞48个,高危漏洞22个,中危漏洞17个,低危漏洞2个,
弱口令账户0个。
通过本次扫描可以看出,扫描的总体状况是极度危险的, 需要针对性的安全加固。
二、安全建议
针对本次扫描结果,特提出如下建议：
1、参考产品提供的漏洞建议和解决方案进行系统安全加固。
2、安全加固的方案有关掉服务、修改密码为强密码、修改系统或服务配置、打补丁、升级软件版本、合理的安全访问策略（如ip地址或端口访问控制）等,请选择合理的安全解决方案。
3、对于关键系统的系统加固,为保证业务运行的连续性,须制定合理的、符合系统特性的加固方案,并且加固方案应通过可行性论证并得到具体的验证。如果必要的话,可以请专门的安全服务机构处理,并和相关厂家进行方案确认。有条件的,也可以通过业务测试环境对加固方案进行评估和检验。
4、对于高风险和关键业务的漏洞要及时进行加固处理。
目前WEB类应用越来越多,其安全威胁日益加剧,建议采用产品自带的WEB扫描模块配合使用。
5、采用本产品进行周期性扫描，定期对资产安全状态进行评估,及时发现漏洞风险，验证安全加固效果。
6、及时更新漏洞库（建议每周进行一次升级）,能够对最新漏洞包括0day进行发现，应对最新漏洞风险。