

# 乌兰浩特市人大常委会办公室安全 评估报告-主机报表

报表生成时间 2022-04-20 16:47:09

---

# 目录

1 主机概况 .....	1
2 漏洞信息 .....	1
3 其他信息 .....	5
4 参考标准 .....	7

## 1 主机概况

主机风险	⚠ 非常危险(10.0分)
IP地址	100.112.0.54
操作系统	Linux 3.10 - 4.11
系统版本	V6.0R04F01SP02
插件版本	V6.0R02F01.2610
扫描起始时间	2022-04-19 15:57:50
扫描结束时间	2022-04-19 15:59:27
漏洞扫描检查模板	自动匹配扫描
漏洞风险评估分	10.0
主机风险评估分	10.0

## 2 漏洞信息

### 2.1 漏洞概况

远程扫描			
端口	协议	服务	漏洞
--	ICMP	--	➡ ICMP timestamp请求响应漏洞
--	UDP	--	➡ 允许Traceroute探测
123	UDP	ntp	➡ 检测到目标主机上运行着NTP服务
3307	TCP	mysql	<ul style="list-style-type: none"><li>➡ Oracle MySQL Server 信息泄露漏洞(CVE-2021-22946)</li><li>➡ Oracle MySQL Server安全漏洞(CVE-2019-17543)</li><li>➡ Oracle MySQL Server 缓冲区溢出漏洞(CVE-2021-3711)</li><li>➡ Oracle MySQL Server 输入验证错误漏洞(CVE-2021-22926)</li><li>➡ Oracle MySQL Server安全漏洞(CVE-2021-22901)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2021-23853)</li><li>⚠ Oracle MySQL 输入验证错误漏洞(CVE-2021-2342)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2021-2372)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21303)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21245)</li><li>⚠ Oracle MySQL/MariaDB Server 输入验证错误漏洞(CVE-2021-35604)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2021-35624)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21367)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21270)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21304)</li><li>⚠ Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21344)</li></ul>

3307	TCP	mysql	<ul style="list-style-type: none"> <li>🚫 Oracle MySQL/MariaDB Server 输入验证错误漏洞 (CVE-2021-2389)</li> <li>🚫 Oracle MySQL Server 输入验证错误漏洞 (CVE-2021-2390)</li> <li>🚫 Oracle MySQL Server 输入验证错误漏洞 (CVE-2021-2356)</li> </ul>
10001	TCP	http	<ul style="list-style-type: none"> <li>🔴 Apache Tomcat 资源管理错误漏洞(CVE-2021-42340)</li> <li>🔴 Apache Tomcat 权限许可和访问控制问题漏洞 (CVE-2022-23181)</li> <li>🚫 Alibaba Druid 未授权访问【原理扫描】</li> <li>🚫 Apache Tomcat 环境问题漏洞(CVE-2021-33037)</li> </ul>

## 2.2 漏洞详情

漏洞名称	🔴 Oracle MySQL Server 信息泄露漏洞(CVE-2021-22946)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在信息泄露漏洞，该漏洞的存在是由于 MySQL Server 中的 Server: Compiling (cURL) 组件存在信息泄露漏洞。攻击者可利用该漏洞未授权读取数据，影响数据的保密性。
解决办法	厂商补丁： Oracle ---- 目前厂商已经发布了升级补丁以修复这个安全问题，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujan2022.html">https://www.oracle.com/security-alerts/cpujan2022.html</a>
威胁分值	7.5
危险插件	否
发现日期	2021-10-25
CVE编号	CVE-2021-22946
NSFOCUS	60265
CNNVD编号	CNNVD-202109-997
CNCVE编号	CNCVE-202122946
CVSS评分	5.0

漏洞名称	🔴 Oracle MySQL Server安全漏洞(CVE-2019-17543)
详细描述	Oracle MySQL是一套开源的关系数据库管理系统。MySQL Server是其中的一个数据库服务器组件。 Oracle MySQL中的Server: Compiling (LZ4)子组件实现中存在安全漏洞。攻击者可利用该漏洞影响数据的可用性。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a>
威胁分值	8.1
危险插件	否
发现日期	2020-07-20
CVE编号	CVE-2019-17543
CNNVD编号	CNNVD-201910-785
CNCVE编号	CNCVE-201917543
CVSS评分	6.8

CNVD编号	CNVD-2020-13556
漏洞名称	🔴 Oracle MySQL Server 缓冲区溢出漏洞(CVE-2021-3711)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于在MySQL服务器的Server: Packaging (OpenSSL)组件中输入验证不正确。远程特权用户可以利用此漏洞获取敏感信息的访问权。该漏洞允许远程特权用户访问敏感信息。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpuoct2021.html">https://www.oracle.com/security-alerts/cpuoct2021.html</a>
威胁分值	9.8
危险插件	否
发现日期	2021-10-19
CVE编号	CVE-2021-3711
CNNVD编号	CNNVD-202108-1945
CNCVE编号	CNCVE-20213711
CVSS评分	7.5
漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2021-22926)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞是由于MySQL服务器中Compiling (cURL)组件的输入验证不正确造成的。远程特权用户可以利用此漏洞破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpuoct2021.html">https://www.oracle.com/security-alerts/cpuoct2021.html</a>
威胁分值	7.5
危险插件	否
发现日期	2021-07-21
CVE编号	CVE-2021-22926
CNNVD编号	CNNVD-202107-1586
CNCVE编号	CNCVE-202122926
CVSS评分	5.0
漏洞名称	🔴 Oracle MySQL Server安全漏洞(CVE-2021-22901)
详细描述	Oracle MySQL是一套开源的关系数据库管理系统。MySQL Server是其中的一个数据库服务器组件。Oracle MySQL Server在Server: Packaging (curl)子组件实现中存在安全漏洞。攻击者可利用该漏洞影响数据的可用性。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a>
威胁分值	8.1
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-22901
CNNVD编号	CNNVD-202105-1683

CNCVE编号	CNCVE-202122901
CVSS评分	6.8

漏洞名称	🔴 Apache Tomcat 资源管理错误漏洞(CVE-2021-42340)
详细描述	Apache Tomcat是美国阿帕奇 ( Apache ) 基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page ( JSP ) 的支持。 Apache Tomcat存在安全漏洞，该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://lists.apache.org/thread.html/r83a35be60f06aca2065f188ee542b9099695d57ced2e70e0885f905c%40%3Cannounce.tomcat.apache.org%3E">https://lists.apache.org/thread.html/r83a35be60f06aca2065f188ee542b9099695d57ced2e70e0885f905c%40%3Cannounce.tomcat.apache.org%3E</a>
威胁分值	7.5
危险插件	否
发现日期	2021-10-14
CVE编号	CVE-2021-42340
CNNVD编号	CNNVD-202110-1057
CNCVE编号	CNCVE-202142340
CVSS评分	5.0

漏洞名称	🔴 Apache Tomcat 权限许可和访问控制问题漏洞(CVE-2022-23181)
详细描述	Apache Tomcat是美国阿帕奇 ( Apache ) 基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page ( JSP ) 的支持。 Apache Tomcat 存在权限许可和访问控制问题漏洞，攻击者可以通过 FileStore Sessions 绕过 Apache Tomcat 的限制，以提升他的权限。 受影响版本： Apache Tomcat 10.1.0-M1 to 10.1.0-M8 Apache Tomcat 10.0.0-M5 to 10.0.14 Apache Tomcat 9.0.35 to 9.0.56 Apache Tomcat 8.5.55 to 8.5.73
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://tomcat.apache.org/security-8.html">https://tomcat.apache.org/security-8.html</a> <a href="https://tomcat.apache.org/security-9.html">https://tomcat.apache.org/security-9.html</a> <a href="https://tomcat.apache.org/security-10.html">https://tomcat.apache.org/security-10.html</a>
威胁分值	7.0
危险插件	否
发现日期	2022-01-26
CVE编号	CVE-2022-23181
CNNVD编号	CNNVD-202201-2423
CNCVE编号	CNCVE-202223181
CVSS评分	4.4
CNVD编号	CNVD-2022-08354

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2021-23853)
------	--

详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于MySQL服务器中的Server：Replication组件内不正确的输入验证。远程特权用户可以利用这个漏洞破坏或删除数据。该漏洞允许远程特权用户破坏或删除数据。
解决办法	厂商补丁： Oracle ----- 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： 链接： <a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a>
威胁分值	5.0
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-2385
CNNVD编号	CNNVD-202107-1465
CNCVE编号	CNCVE-20212385
CVSS评分	4.9
CNVD编号	CNVD-2021-54676

漏洞名称	🔴 Oracle MySQL 输入验证错误漏洞(CVE-2021-2342)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。Oracle MySQL 存在输入验证错误漏洞，该漏洞源于MySQL服务器中的Server: Optimizer组件内不正确的输入验证。远程特权用户可以利用这个漏洞执行拒绝服务(DoS)攻击。以下产品和版本的影响:MySQL服务器:5.7.0,5.7.1,5.7.2,5.7.3,5.7.4,5.7.5,5.7.6,5.7.7,5.7.8,5.7.9,5.7.10,5.7.11,5.7.12,5.7.13,5.7.14,5.7.15,5.7.16,5.7.17,5.7.18,5.7.19,5.7.20,5.7.21,5.7.22,5.7.23,5.7.24,5.7.25,5.7.26,5.7.27,5.7.28,5.7.29,
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a>
威胁分值	4.9
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-2342
CNNVD编号	CNNVD-202107-1387
CNCVE编号	CNCVE-20212342
CVSS评分	4
CNVD编号	CNVD-2021-54390

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2021-2372)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。Oracle MySQL/MariaDB Server 中存在输入验证错误漏洞，该漏洞源于产品的InnoDB组件未能正确处理用户输入数据。攻击者可通过该漏洞引起拒绝服务攻击。以下产品及版本受到影响：Oracle MySQL Server 5.7.0版本至5.7.34版本，Oracle MySQL Server 8.0.0至8.0.25版本，MariaDB 10.6.4之前版本，MariaDB 10.5.12之前版本，MariaDB 10.4.21之前版本，MariaDB 10.3.31之前版本，MariaDB 10.2.40之前版本。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： <a href="https://www.oracle.com/">https://www.oracle.com/</a>

威胁分值	4.4
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-2372
CNNVD编号	CNNVD-202107-1455
CNCVE编号	CNCVE-20212372
CVSS评分	3.5
CNVD编号	CNVD-2021-54027

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21303)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server 存在输入验证错误漏洞，该漏洞源于 MySQL Server 中的 Server: Stored Procedure 组件中的输入验证不正确。远程特权用户可以利用此漏洞执行拒绝服务 (DoS) 攻击。该漏洞允许远程特权用户执行拒绝服务 (DoS) 攻击。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujan2022.html">https://www.oracle.com/security-alerts/cpujan2022.html</a>
威胁分值	4.9
危险插件	否
发现日期	2022-01-18
CVE编号	CVE-2022-21303
CNNVD编号	CNNVD-202201-1429
CNCVE编号	CNCVE-202221303
CVSS评分	4.0

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21245)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于 MySQL Server 中的 Server: Optimizer 组件中的输入验证不正确。远程认证用户可以利用此漏洞破坏或删除数据。该漏洞允许远程认证用户破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.cybersecurity-help.cz/vdb/SB2022011905">https://www.cybersecurity-help.cz/vdb/SB2022011905</a>
威胁分值	4.3
危险插件	否
发现日期	2022-01-19
CVE编号	CVE-2022-21245
CNNVD编号	CNNVD-202201-1611
CNCVE编号	CNCVE-202221245
CVSS评分	4.0
CNVD编号	CNVD-2022-09144

漏洞名称	🔴 Oracle MySQL/MariaDB Server 输入验证错误漏洞(CVE-2021-35604)
------	--



详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL/MariaDB Server存在输入验证错误漏洞，该漏洞是由于MySQL/MariaDB服务器中InnoDB组件的输入验证不正确造成的。远程特权用户可以利用此漏洞破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpuoct2021.html">https://www.oracle.com/security-alerts/cpuoct2021.html</a>
威胁分值	5.5
危险插件	否
发现日期	2021-10-19
CVE编号	CVE-2021-35604
CNNVD编号	CNNVD-202110-1333
CNCVE编号	CNCVE-202135604
CVSS评分	5.5
CNVD编号	CNVD-2021-81783

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2021-35624)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于在MySQL服务器的Server: Security: Privileges组件中输入验证不正确。远程特权用户可以利用此漏洞操纵数据。该漏洞允许远程特权用户操纵数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpuoct2021.html">https://www.oracle.com/security-alerts/cpuoct2021.html</a>
威胁分值	4.9
危险插件	否
发现日期	2021-10-19
CVE编号	CVE-2021-35624
CNNVD编号	CNNVD-202110-1303
CNCVE编号	CNCVE-202135624
CVSS评分	4
CNVD编号	CNVD-2021-81769

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21367)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于MySQL Server 中的Server: Optimizer 组件中的输入验证不正确。远程认证用户可以利用此漏洞破坏或删除数据。该漏洞允许远程认证用户破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.cybersecurity-help.cz/vdb/SB2022011905">https://www.cybersecurity-help.cz/vdb/SB2022011905</a>
威胁分值	5.5
危险插件	否
发现日期	2022-01-19
CVE编号	CVE-2022-21367
CNNVD编号	CNNVD-202201-1594

CNCVE编号	CNCVE-202221367
CVSS评分	5.5
CNVD编号	CNVD-2022-17681

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21270)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于 MySQL Server 中的 Server: Optimizer 组件中的输入验证不正确。远程认证用户可以利用此漏洞破坏或删除数据。该漏洞允许远程认证用户破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.cybersecurity-help.cz/vdb/SB2022011905">https://www.cybersecurity-help.cz/vdb/SB2022011905</a>
威胁分值	4.9
危险插件	否
发现日期	2022-01-19
CVE编号	CVE-2022-21270
CNNVD编号	CNNVD-202201-1599
CNCVE编号	CNCVE-202221270
CVSS评分	4.0
CNVD编号	CNVD-2022-09135

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21304)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。Oracle MySQL Server 存在输入验证错误漏洞，该漏洞源于 MySQL Server 中的 Server: Parser 组件中的输入验证不正确。远程特权用户可以利用此漏洞执行拒绝服务 (DoS) 攻击。该漏洞允许远程特权用户执行拒绝服务 (DoS) 攻击。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujan2022.html">https://www.oracle.com/security-alerts/cpujan2022.html</a>
威胁分值	4.9
危险插件	否
发现日期	2022-01-18
CVE编号	CVE-2022-21304
CNNVD编号	CNNVD-202201-1430
CNCVE编号	CNCVE-202221304
CVSS评分	4.0
CNVD编号	CNVD-2022-17694

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2022-21344)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于 MySQL Server 中的 Server: Optimizer 组件中的输入验证不正确。远程认证用户可以利用此漏洞破坏或删除数据。该漏洞允许远程认证用户破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.cybersecurity-help.cz/vdb/SB2022011905">https://www.cybersecurity-help.cz/vdb/SB2022011905</a>

威胁分值	4.9
危险插件	否
发现日期	2022-01-19
CVE编号	CVE-2022-21344
CNNVD编号	CNNVD-202201-1608
CNCVE编号	CNCVE-202221344
CVSS评分	4.0
CNVD编号	CNVD-2022-17685

漏洞名称	🔴 Oracle MySQL/MariaDB Server 输入验证错误漏洞(CVE-2021-2389)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL/MariaDB Server 存在输入验证错误漏洞，该漏洞源于MySQL的InnoDB组件内部输入验证不当，远程未经身份验证的攻击者可利用该漏洞执行拒绝服务攻击。
解决办法	厂商补丁： Oracle ----- 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a>
威胁分值	5.9
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-2389
CNNVD编号	CNNVD-202107-1355
CNCVE编号	CNCVE-20212389
CVSS评分	7.1
CNVD编号	CNVD-2021-54679

漏洞名称	🔴 Oracle MySQL Server 输入验证错误漏洞(CVE-2021-2390)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server存在输入验证错误漏洞，该漏洞的存在是由于MySQL服务器的InnoDB组件内部输入验证不当。远程未经身份验证的攻击者可利用该漏洞可以利用这个漏洞执行拒绝服务(DoS)攻击。该漏洞允许远程未经身份验证的攻击者可利用该漏洞执行拒绝服务(DoS)攻击。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页： <a href="https://www.oracle.com">https://www.oracle.com</a>
威胁分值	5.9
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-2390
CNNVD编号	CNNVD-202107-1461
CNCVE编号	CNCVE-20212390
CVSS评分	7.1
CNVD编号	CNVD-2021-54678

漏洞名称	🚫 Oracle MySQL Server 输入验证错误漏洞(CVE-2021-2356)
详细描述	Oracle MySQL Server是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server 存在输入验证错误漏洞，该漏洞源于MySQL Server中的Server:Replication组件内不正确的输入验证，通过身份验证的远程用户可以利用此漏洞破坏或删除数据。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://www.oracle.com/security-alerts/cpujul2021.html">https://www.oracle.com/security-alerts/cpujul2021.html</a> 。
威胁分值	5.9
危险插件	否
发现日期	2021-07-20
CVE编号	CVE-2021-2356
CNNVD编号	CNNVD-202107-1374
CNCVE编号	CNCVE-20212356
CVSS评分	4.9
CNVD编号	CNVD-2021-57181

漏洞名称	🚫 Alibaba Druid 未授权访问【原理扫描】
详细描述	Alibaba Druid是一款Java语言开发的数据库连接池。Druid能够提供强大的监控和扩展功能。 Alibaba Druid 默认情况下未设置访问控制，攻击者可以登录以获取敏感信息
解决办法	对druid进行权限配置
威胁分值	5.0
危险插件	否
发现日期	2021-04-16

漏洞名称	🚫 Apache Tomcat 环境问题漏洞(CVE-2021-33037)
详细描述	Apache Tomcat是美国阿帕奇（Apache）基金会的一款轻量级Web应用服务器。该程序实现了对Servlet和JavaServer Page（JSP）的支持。 Apache Tomcat存在环境问题漏洞，该漏洞源于Apache Tomcat 在某些情况下没有正确解析 HTTP 传输编码请求标头，导致在与反向代理一起使用时可能会请求走私。
解决办法	厂商补丁： 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： <a href="https://camel.apache.org/security/">https://camel.apache.org/security/</a> <a href="https://tomcat.apache.org/security-8.html">https://tomcat.apache.org/security-8.html</a> <a href="https://tomcat.apache.org/security-9.html">https://tomcat.apache.org/security-9.html</a> <a href="https://tomcat.apache.org/security-10.html">https://tomcat.apache.org/security-10.html</a>
威胁分值	5.3
危险插件	否
发现日期	2021-07-12
CVE编号	CVE-2021-33037
CNNVD编号	CNNVD-202107-681
CNCVE编号	CNCVE-202133037
CVSS评分	5

漏洞名称	🟢 ICMP timestamp请求响应漏洞
------	------------------------

详细描述	远程主机回复ICMP_TIMESTAMP查询并返回它们系统的当前时间。这可能允许攻击者攻击一些基于时间认证的协议。
解决办法	NSFOCUS建议您采取以下措施以降低威胁： * 在您的防火墙上过滤外来的ICMP timestamp（类型 13）报文以及外出的ICMP timestamp回复报文。
威胁分值	2.1
危险插件	否
发现日期	1997-08-01
CVE编号	CVE-1999-0524
CNNVD编号	CNNVD-199708-003
CNCVE编号	CNCVE-19990524
CVSS评分	0

漏洞名称	🟢 允许Traceroute探测
详细描述	本插件使用Traceroute探测来获取扫描器与远程主机之间的路由信息。攻击者也可以利用这些信息来了解目标网络的网络拓扑。
解决办法	在防火墙出站规则中禁用echo-reply（type 0）、time-exceeded（type 11）、destination-unreachable（type 3）类型的ICMP包。
威胁分值	1.0
危险插件	否
发现日期	1999-01-01

漏洞名称	🟢 检测到目标主机上运行着NTP服务
详细描述	通过NTP查询可以获取远端主机很多信息，包括操作系统、当前时间等。如果不是十分必要，应该禁用该服务。
解决办法	由于该服务对于常规应用来说并无必要，NSFocus建议您关闭NTPD。
威胁分值	0.0
危险插件	否
发现日期	2001-01-01

## 3 其它信息

### 3.1 远程端口信息

端口	协议	服务	状态
123	udp	ntp	open
3307	tcp	mysql	open
10001	tcp	http	open

### 3.2 操作系统类型




操作系统名字	版本号
Linux	3.10 - 4.11

### 3.3 端口Banner

端口	Banner
3307	MySQL/5.7.34
10001	Apache Tomcat/9.0.46

## 4 参考标准

### 4.1 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	$7 \leq \text{漏洞风险值} \leq 10$	攻击者可以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	$4 \leq \text{漏洞风险值} < 7$	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	$0 \leq \text{漏洞风险值} < 4$	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。

说明：

漏洞的风险值兼容CVSS评分标准。

### 4.2 主机风险等级评定标准

主机风险等级	主机风险值区域
 非常危险	$7.0 \leq \text{主机风险值} \leq 10.0$
 比较危险	$5.0 \leq \text{主机风险值} < 7.0$
 比较安全	$2.0 \leq \text{主机风险值} < 5.0$
 非常安全	$0.0 \leq \text{主机风险值} < 2.0$

说明：

1. 按照远程安全评估系统的主机风险评估模型计算主机风险值。根据得到的主机风险值参考“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值范围。