"远程安全评估系统"安全评估报告-主机报表

报表生成时间 2024-10-30 16:12:27

目录

1 主机概况

主机风险	非常危险(10.0分)
IP地址	10.2.111.18
操作系统	Linux 3.10 - 4.11
系统版本	V6.0R04F03SP04
插件版本	V6.0R02F01.3800
扫描起始时间	2024-10-26 14:33:25
扫描结束时间	2024-10-26 15:29:35
漏洞扫描检查模板	全部漏洞扫描
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**
22	TCP	ssh	SSH版本信息可被获取 探测到SSH服务器支持的算法
443	TCP	https	可通过HTTP获取远端WWW服务信息 获取目标SSL证书过期时间【原理扫描】 获取SSL 证书中的hostname【原理扫描】 检测到目标主机加密通信支持的SSL加密算法【原理扫描】 探测到服务器支持的SSL加密协议【原理扫描】
3306	TCP	mysql	Oracle MySQL cURL 组件输入验证错误漏洞 (CVE-2022-42916) Oracle MySQL cURL 组件输入验证错误漏洞 (CVE-2022-32221) Oracle MySQL 安全漏洞(CVE-2023-0215) Oracle MySQL curl安全漏洞(CVE-2022-43551) Oracle MySQL 安全漏洞(CVE-2023-21980) Oracle MySQL zlib安全漏洞(CVE-2022-37434) Oracle MySQL 安全漏洞(CVE-2023-21912) Oracle MySQL curl/libcURL 安全漏洞 (CVE-2023-38545) Oracle MySQL Server 安全漏洞(CVE-2023-0464) Oracle MySQL 安全漏洞(CVE-2022-4450) Oracle MySQL 安全漏洞(CVE-2023-0286) Oracle MySQL cURL 组件输入验证错误漏洞 (CVE-2022-42915) Oracle MySQL 安全漏洞(CVE-2023-22028) Oracle MySQL 安全漏洞(CVE-2022-4304) Oracle MySQL Server 安全漏洞(CVE-2023-0466) Oracle MySQL Server 安全漏洞(CVE-2023-1255)

3306	TCP	mysql	Oracle MySQL Server 安全漏洞(CVE-2023-22015) Oracle MySQL 安全漏洞(CVE-2023-22026) Oracle MySQL 安全漏洞(CVE-2023-22053) Oracle MySQL 安全漏洞(CVE-2023-22007) Oracle MySQL cURL 组件输入验证错误漏洞(CVE-2022-35260) Oracle MySQL Server 安全漏洞(CVE-2023-22084) Oracle MySQL Server 安全漏洞(CVE-2023-2650) Oracle MySQL Server 安全漏洞(CVE-2023-0465) Oracle MySQL 安全漏洞(CVE-2022-21592) Oracle MySQL 安全漏洞(CVE-2022-21589) Oracle MySQL 安全漏洞(CVE-2022-21617) Oracle MySQL 安全漏洞(CVE-2022-21608) Oracle MySQL OpenSSL组件安全漏洞（CVE-2022-2097） Oracle MySQL 安全漏洞(CVE-2023-21840) Oracle MySQL 安全漏洞(CVE-2023-21963) Oracle MySQL curl/libcURL 安全漏洞(CVE-2023-38546)
3306	TCP	mysql	可以获取到MySQL/MariaDB/Percona/TiDB Server版本信息 远程MySQL/MariaDB/Percona/TiDB Server版本泄露
8000	TCP	http	可通过HTTP获取远端WWW服务信息
8082	TCP	www	Apache Tomcat 安全漏洞(CVE-2024-34750) Apache Tomcat 注入漏洞(CVE-2022-45143) Apache Tomcat 拒绝服务漏洞(CVE-2023-24998) Apache Tomcat 输入验证错误漏洞(CVE-2023-46589) Apache Tomcat 环境问题漏洞(CVE-2022-42252) HTTP/2拒绝服务漏洞（CVE-2023-44487） Apache Tomcat 输入验证错误漏洞(CVE-2023-41080) Apache Tomcat文件包含漏洞(CVE-2023-28708) Apache Tomcat 安全漏洞(CVE-2023-42795) Apache Tomcat 输入验证错误漏洞(CVE-2023-45648) Apache Tomcat 输入验证错误漏洞(CVE-2024-24549) Apache Tomcat 安全漏洞(CVE-2024-23672) 可通过HTTP获取远端WWW服务信息
8095	TCP	www	获取目标SSL证书过期时间【原理扫描】 获取SSL 证书中的hostname【原理扫描】 检测到目标主机加密通信支持的SSL加密算法【原理扫描】
8888	TCP	http	可通过HTTP获取远端WWW服务信息

2.2 漏洞详情

漏洞名称	Oracle MySQL cURL 组件输入验证错误漏洞(CVE-2022-42916)
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 5.7.40及之前版本，8.0.31及之前版本存在输入验证错误漏洞，该漏洞源于MySQL Server中的Server: Packaging (cURL)组件内不正确的输入验证。
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： https://www.oracle.com/security-alerts/cpujan2023.html
威胁分值	7.5
危险插件	否
发现日期	2023-01-17
CVE编号	CVE-2022-42916

CNNVD编号	CNNVD-202210-2216
CNCVE编号	CNCVE-202242916

漏洞名称	Oracle MySQL cURL 组件输入验证错误漏洞(CVE-2022-32221)
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 5.7.40及之前版本，8.0.31及之前版本存在输入验证错误漏洞，该漏洞源于MySQL Server中的Server: Packaging (cURL)组件内不正确的输入验证。
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： https://www.oracle.com/security-alerts/cpujan2023.html
威胁分值	9.8
危险插件	否
发现日期	2023-01-17
CVE编号	CVE-2022-32221
CNNVD编号	CNNVD-202210-2214
CNCVE编号	CNCVE-202232221

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-0215)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。 Oracle MySQL 5.7.41及之前版本，8.0.32及版本及之前版本的Server: Packaging (OpenSSL)组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	7.5
危险插件	否
发现日期	2023-04-18
CVE编号	CVE-2023-0215
CNNVD编号	CNNVD-202302-521
CNCVE编号	CNCVE-20230215

漏洞名称	Oracle MySQL curl安全漏洞(CVE-2022-43551)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。 Oracle MySQL 5.7.41 版本及之前版本和 8.0.32 版本及之前版本的 Server: Server: Packaging (cURL) 组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	7.5
危险插件	否
发现日期	2023-04-19
CVE编号	CVE-2022-43551
CNNVD编号	CNNVD-202212-3665
CNCVE编号	CNCVE-202243551

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-21980)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的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 5.7.41 版本及之前版本和 8.0.32 版本及之前版本的 Client programs 组件存在安全漏洞。低权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	7.1
危险插件	否
发现日期	2023-04-18
CVE编号	CVE-2023-21980
CNNVD编号	CNNVD-202304-1478
CNCVE编号	CNCVE-202321980
CNVD编号	CNVD-2023-65514

漏洞名称	Oracle MySQL zlib安全漏洞(CVE-2022-37434)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL 5.7.41版本及之前版本和 8.0.31 版本及之前版本的 Server: InnoDB (zlib)组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	9.8
危险插件	否
发现日期	2023-04-19
CVE编号	CVE-2022-37434
CNNVD编号	CNNVD-202208-2276
CNCVE编号	CNCVE-202237434

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-21912)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL 5.7.41 版本及之前版本和 8.0.30 版本及之前版本的 Server: Security: Privileges 组件存在安全漏洞。未经身份验证的攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	7.5
危险插件	否
发现日期	2023-04-18
CVE编号	CVE-2023-21912
CNNVD编号	CNNVD-202304-1533
CNCVE编号	CNCVE-202321912

CNVD编号	CNVD-2023-67104

漏洞名称	Oracle MySQL curl/libcURL 安全漏洞(CVE-2023-38545)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL Server 5.7.43及之前版本，8.0.34及之前版本和8.1.0存在安全漏洞，该漏洞源于MySQL Server中的Server: Compiling (curl)组件允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	9.8
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-38545
CNNVD编号	CNNVD-202310-917
CNCVE编号	CNCVE-202338545
CNVD编号	CNVD-2023-75809

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-0464)
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 5.7.42及之前版本和8.0.33及之前版本存在安全漏洞，该漏洞源于允许低权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	7.5
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-0464
CNNVD编号	CNNVD-202303-1681
CNCVE编号	CNCVE-20230464

漏洞名称	Oracle MySQL 安全漏洞(CVE-2022-4450)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL 5.7.41及之前版本，8.0.32及版本及之前版本的Server: Packaging (OpenSSL)组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	7.5
危险插件	否
发现日期	2023-02-07
CVE编号	CVE-2022-4450
CNNVD编号	CNNVD-202302-510
CNCVE编号	CNCVE-20224450

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-0286)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。 Oracle MySQL 5.7.41及之前版本，8.0.32及版本及之前版本的Server: Packaging (OpenSSL)组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	7.4
危险插件	否
发现日期	2023-02-07
CVE编号	CVE-2023-0286
CNNVD编号	CNNVD-202302-524
CNCVE编号	CNCVE-20230286

漏洞名称	Oracle MySQL cURL 组件输入验证错误漏洞(CVE-2022-42915)
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 5.7.40及之前版本，8.0.31及之前版本存在输入验证错误漏洞，该漏洞源于MySQL Server中的Server: Packaging (cURL)组件内不正确的输入验证。
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： https://www.oracle.com/security-alerts/cpujan2023.html
威胁分值	8.1
危险插件	否
发现日期	2023-01-17
CVE编号	CVE-2022-42915
CNNVD编号	CNNVD-202210-2217
CNCVE编号	CNCVE-202242915

漏洞名称	Apache Tomcat 安全漏洞(CVE-2024-34750)
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，该漏洞源于存在异常情况处理不当、资源消耗不受控制的漏洞。
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: https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvplnl77y8l
威胁分值	7.5
危险插件	否
发现日期	2024-07-03
CVE编号	CVE-2024-34750
CNNVD编号	CNNVD-202407-326
CNCVE编号	CNCVE-202434750

漏洞名称	Apache Tomcat 注入漏洞(CVE-2022-45143)

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 8.5.83版本、9.0.40版本至9.0.68版本、10.1.0-M1版本至10.1.1版本存在注入漏洞，该漏洞源于JsonErrorReportValve没有转义类型、消息或描述值。
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： https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj
威胁分值	7.5
危险插件	否
发现日期	2023-01-03
CVE编号	CVE-2022-45143
CNNVD编号	CNNVD-202301-137
CNCVE编号	CNCVE-202245143

漏洞名称	Apache Tomcat 拒绝服务漏洞(CVE-2023-24998)
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使用Apache Commons FileUpload的打包重命名副本来提供Jakarta Servlet规范中定义的文件上传功能。因此，Apache Tomcat也容易受到Apache Commons FileUpload漏洞CVE-2023-24998的攻击，因为处理的请求部分数量没有限制。这导致攻击者有可能通过恶意上传或一系列上传触发DoS。
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： https://tomcat.apache.org/security-9.html
威胁分值	7.5
危险插件	否
发现日期	2023-02-20
CVE编号	CVE-2023-24998
CNNVD编号	CNNVD-202302-1610
CNCVE编号	CNCVE-202324998
CNVD编号	CNVD-2023-23552

漏洞名称	Apache Tomcat 输入验证错误漏洞(CVE-2023-46589)
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存在输入验证错误漏洞，该漏洞源于存在不正确的输入验证漏洞，可能会导致将单个请求视为多个请求，从而在反向代理后面出现请求走私。
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: https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr
威胁分值	7.5
危险插件	否
发现日期	2023-11-28
CVE编号	CVE-2023-46589
CNNVD编号	CNNVD-202311-2168
CNCVE编号	CNCVE-202346589

漏洞名称	Apache Tomcat 环境问题漏洞(CVE-2022-42252)
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，该漏洞源于当 rejectIllegalHeader 设置为 false 时，Tomcat 可能存在请求走私问题（Request Smuggling）。
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： https://tomcat.apache.org/security-8.html https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-10.html
威胁分值	7.5
危险插件	否
发现日期	2022-10-31
CVE编号	CVE-2022-42252
CNNVD编号	CNNVD-202210-2602
CNCVE编号	CNCVE-202242252
CNVD编号	CNVD-2022-74082

漏洞名称	HTTP/2拒绝服务漏洞（CVE-2023-44487）
详细描述	HTTP/2是超文本传输协议或HTTP，浏览器用于与Web服务器通信。 HTTP/2存在拒绝服务漏洞，攻击者可利用该漏洞导致目标系统停止响应。
解决办法	厂商补丁: 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： https://lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwhsjlsd87q
威胁分值	7.5
危险插件	否
发现日期	2023-10-12
CVE编号	CVE-2023-44487
CNNVD编号	CNNVD-202310-667
CNCVE编号	CNCVE-202344487
CNVD编号	CNVD-2023-75597

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-22028)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL Server 5.7.43及之前版本，8.0.31及之前版本存在安全漏洞存在安全漏洞，该漏洞源于允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	4.9
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-22028
CNNVD编号	CNNVD-202310-1369

CNCVE编号	CNCVE-202322028

漏洞名称	Oracle MySQL 安全漏洞(CVE-2022-4304)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL 5.7.41及之前版本，8.0.32及版本及之前版本的Server: Packaging (OpenSSL)组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	5.9
危险插件	否
发现日期	2023-02-07
CVE编号	CVE-2022-4304
CNNVD编号	CNNVD-202302-514
CNCVE编号	CNCVE-20224304

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-0466)
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 5.7.42及之前版本和8.0.33及之前版本存在安全漏洞，该漏洞源于允许低权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	5.3
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-0466
CNNVD编号	CNNVD-202303-2431
CNCVE编号	CNCVE-20230466

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-1255)
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 5.7.42及之前版本和8.0.33及之前版本存在安全漏洞，该漏洞源于允许低权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	5.9
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-1255
CNNVD编号	CNNVD-202304-1714
CNCVE编号	CNCVE-20231255

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-22015)

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 5.7.42及之前版本，8.0.31及之前版本存在安全漏洞，该漏洞源于允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	4.9
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-22015
CNNVD编号	CNNVD-202310-1361
CNCVE编号	CNCVE-202322015

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-22026)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。 Oracle MySQL Server 5.7.42及之前版本，8.0.31及之前版本存在安全漏洞，该漏洞源于允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	4.9
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-22026
CNNVD编号	CNNVD-202310-1368
CNCVE编号	CNCVE-202322026

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-22053)
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 的 MySQL Server product 存在安全漏洞，该漏洞源于 Client programs 模块允许低权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。成功攻击此漏洞可能会导致未经授权的能力导致 MySQL 服务器挂起或频繁重复崩溃（完整的 DOS），以及对 MySQL 服务器可访问数据的子集进行未经授权的读取访问。
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： https://www.oracle.com/security-alerts/cpujul2023.html
威胁分值	5.9
危险插件	否
发现日期	2023-07-18
CVE编号	CVE-2023-22053
CNNVD编号	CNNVD-202307-1621
CNCVE编号	CNCVE-202322053
CNVD编号	CNVD-2023-65510

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-22007)

详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。 Oracle MySQL 的 MySQL Server product 存在安全漏洞，该漏洞源于 Server : Replication 模块允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。成功攻击此漏洞可能会导致未经授权的 MySQL 服务器挂起或频繁重复崩溃（完整的 DOS）。
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： https://www.oracle.com/security-alerts/cpujul2023.html
威胁分值	4.9
危险插件	否
发现日期	2023-07-18
CVE编号	CVE-2023-22007
CNNVD编号	CNNVD-202307-1581
CNCVE编号	CNCVE-202322007
CNVD编号	CNVD-2023-65505

漏洞名称	Oracle MySQL cURL 组件输入验证错误漏洞(CVE-2022-35260)
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 5.7.40及之前版本，8.0.31及之前版本存在输入验证错误漏洞，该漏洞源于MySQL Server中的Server: Packaging (cURL)组件内不正确的输入验证。
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： https://www.oracle.com/security-alerts/cpujan2023.html
威胁分值	6.5
危险插件	否
发现日期	2023-01-17
CVE编号	CVE-2022-35260
CNNVD编号	CNNVD-202210-2210
CNCVE编号	CNCVE-202235260
CNVD编号	CNVD-2023-63201

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-22084)
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 5.7.43及之前版本，8.0.34及之前版本和8.1.0存在安全漏洞，该漏洞源于MySQL Server中的Server: Compiling (InnoDB)组件允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	4.9
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-22084
CNNVD编号	CNNVD-202310-1391
CNCVE编号	CNCVE-202322084

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-2650)
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 5.7.42及之前版本，8.0.33及之前版本存在安全漏洞，该漏洞源于允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	6.5
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-2650
CNNVD编号	CNNVD-202305-2503
CNCVE编号	CNCVE-20232650

漏洞名称	Oracle MySQL Server 安全漏洞(CVE-2023-0465)
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 5.7.42及之前版本和8.0.33及之前版本存在安全漏洞，该漏洞源于允许低权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html
威胁分值	5.3
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-0465
CNNVD编号	CNNVD-202303-2432
CNCVE编号	CNCVE-20230465

漏洞名称	Oracle MySQL 安全漏洞(CVE-2022-21592)
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: Encryption组件中输入验证不正确。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： https://www.oracle.com/security-alerts/cpuoct2022.html
威胁分值	4.3
危险插件	否
发现日期	2022-10-18
CVE编号	CVE-2022-21592
CNNVD编号	CNNVD-202210-1289
CNCVE编号	CNCVE-202221592

漏洞名称	Oracle MySQL 安全漏洞(CVE-2022-21589)

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： https://www.oracle.com/security-alerts/cpuoct2022.html
威胁分值	4.3
危险插件	否
发现日期	2022-10-18
CVE编号	CVE-2022-21589
CNNVD编号	CNNVD-202210-1284
CNCVE编号	CNCVE-202221589

漏洞名称	Oracle MySQL 安全漏洞(CVE-2022-21617)
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/MariaDB 在Server: Connection Handling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机密性、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： https://www.oracle.com/security-alerts/cpuoct2022.html
威胁分值	4.9
危险插件	否
发现日期	2022-10-18
CVE编号	CVE-2022-21617
CNNVD编号	CNNVD-202210-1292
CNCVE编号	CNCVE-202221617
CNVD编号	CNVD-2022-89431

漏洞名称	Oracle MySQL 安全漏洞(CVE-2022-21608)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的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: Optimizer组件中输入验证不当造成的。本地特权用户可以利用此漏洞进行DoS (denial of service)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： https://www.oracle.com/security-alerts/cpuoct2022.html
威胁分值	4.9
危险插件	否
发现日期	2022-10-18
CVE编号	CVE-2022-21608
CNNVD编号	CNNVD-202210-1316
CNCVE编号	CNCVE-202221608
CNVD编号	CNVD-2022-89435

漏洞名称	Oracle MySQL OpenSSL组件安全漏洞（CVE-2022-2097）
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的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。MySQL Connectors是其中的一个连接使用MySQL的应用程序的驱动程序。 Oracle MySQL（组件：OpenSSL）的 MySQL 服务器产品中存在缓冲区错误漏洞，该漏洞允许通过多种协议进行网络访问的高权限攻击者破坏 MySQL 服务器。成功攻击此漏洞可能导致未经授权的能力导致 MySQL Server 的部分拒绝服务（部分 DOS）。
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： https://www.oracle.com/security-alerts/cpuoct2022.html
威胁分值	5.3
危险插件	否
发现日期	2022-07-05
CVE编号	CVE-2022-2097
CNNVD编号	CNNVD-202207-379
CNCVE编号	CNCVE-20222097
CVSS评分	5.0

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-21840)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。 Oracle MySQL 5.7.40及之前版本存在安全漏洞，攻击者可利用该漏洞致未经授权的能力导致 MySQL 服务器挂起或频繁重复崩溃（完全 DOS）。
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： https://www.oracle.com/security-alerts/cpujan2023.html
威胁分值	4.9
危险插件	否
发现日期	2023-01-18
CVE编号	CVE-2023-21840
CNNVD编号	CNNVD-202301-1367
CNCVE编号	CNCVE-202321840
CNVD编号	CNVD-2023-07924

漏洞名称	Apache Tomcat 输入验证错误漏洞(CVE-2023-41080)
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存在输入验证错误漏洞，该漏洞源于FORM身份验证功能存在开放重定向漏洞，允许攻击者将URL重定向到不受信任站点。受影响的产品和版本： Apache Tomcat 11.0.0-M1至11.0.0-M10版本，10.1.0-M1至10.1.12版本，9.0.0-M1至9.0.79版本，8.5.0 至8.5.92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，补丁获取链接: https://lists.apache.org/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f
威胁分值	6.1
危险插件	否

发现日期	2023-08-25
CVE编号	CVE-2023-41080
CNNVD编号	CNNVD-202308-2096
CNCVE编号	CNCVE-202341080
CNVD编号	CNVD-2023-80565

漏洞名称	Apache Tomcat文件包含漏洞(CVE-2023-28708)
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，该漏洞源于用户代理能通过不安全的通道传输会话cookie导致信息泄露。以下产品和版本收到影响： Apache Tomcat 11.0.0-M1 至 11.0.0-M2版本， Apache Tomcat 10.1.0-M1 至 10.1.5版本， Apache Tomcat 9.0.0-M1 至 9.0.71版本， Apache Tomcat 8.5.0 至 8.5.85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，补丁获取链接： https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67 或者请随时关注如下链接进行更新 http://tomcat.apache.org/security-9.html http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html
威胁分值	4.3
危险插件	否
发现日期	2023-03-22
CVE编号	CVE-2023-28708
CNNVD编号	CNNVD-202303-1662
CNCVE编号	CNCVE-202328708

漏洞名称	Apache Tomcat 安全漏洞(CVE-2023-42795)
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，该漏洞源于回收内部对象时存在安全漏洞，导致请求/响应信息泄露。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M11版本，10.1.0-M1至10.1.13版本，9.0.0-M1至9.0.80版本，8.5.0至8.5.93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，补丁获取链接: https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw
威胁分值	5.3
危险插件	否
发现日期	2023-10-10
CVE编号	CVE-2023-42795
CNNVD编号	CNNVD-202310-716
CNCVE编号	CNCVE-202342795

漏洞名称	Apache Tomcat 输入验证错误漏洞(CVE-2023-45648)

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，该漏洞源于没有正确解析HTTP尾部标头，导致攻击者可以利用特制的尾部标头造成反向代理走私。受影响的产品和版本：Apache Tomcat 11.0.0-M1至11.0.0-M11版本，10.1.0-M1至10.1.13版本，9.0.0.M1至9.0.81版本，8.5.0至8.5.93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，补丁获取链接: https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp
威胁分值	5.3
危险插件	否
发现日期	2023-10-10
CVE编号	CVE-2023-45648
CNNVD编号	CNNVD-202310-712
CNCVE编号	CNCVE-202345648
CNVD编号	CNVD-2024-27498

漏洞名称	Apache Tomcat 输入验证错误漏洞(CVE-2024-24549)
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存在输入验证错误漏洞，该漏洞源于HTTP/2请求的输入验证不正确，会导致拒绝服务。
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: https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg
威胁分值	6.5
危险插件	否
发现日期	2024-03-13
CVE编号	CVE-2024-24549
CNNVD编号	CNNVD-202403-1179
CNCVE编号	CNCVE-202424549
CNVD编号	CNVD-2024-13568

漏洞名称	Apache Tomcat 安全漏洞(CVE-2024-23672)
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，该漏洞源于不完全清理，会导致拒绝服务。
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: https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f
威胁分值	6.5
危险插件	否
发现日期	2024-03-13
CVE编号	CVE-2024-23672
CNNVD编号	CNNVD-202403-1180
CNCVE编号	CNCVE-202423672

CNVD编号	CNVD-2024-13569

漏洞名称	SSH版本信息可被获取
详细描述	SSH服务允许远程攻击者获得ssh的具体信息，如版本号等等。这可能为攻击者发动进一步攻击提供帮助。
解决办法	如果banner包含敏感信息，NSFOCUS建议您采取以下几类措施以降低威胁： * 修改源代码或者配置文件改变SSH服务的缺省banner。 * 配置防火墙策略，阻断ssh banner信息外泄。 如果已经采取了以上几类措施，则表明该漏洞已经不具备暴露敏感信息风险，可以不用修复。
威胁分值	0.0
危险插件	否
发现日期	1999-01-01
CVE编号	CVE-1999-0634
CNCVE编号	CNCVE-19990634

漏洞名称	探测到SSH服务器支持的算法
详细描述	本插件用来获取SSH服务器支持的算法列表
解决办法	
威胁分值	0.0
危险插件	否
发现日期	2016-03-08

漏洞名称	可通过HTTP获取远端WWW服务信息
详细描述	本插件检测远端HTTP Server信息。这可能使得攻击者了解远程系统类型以便进行下一步的攻击。
解决办法	该漏洞仅是为了信息获取，建议隐藏敏感信息。如果banner未包含敏感信息，则表明该漏洞已经不具备暴露敏感信息风险，可以不用修复。
威胁分值	0.0
危险插件	否
发现日期	1999-01-01

漏洞名称	获取目标SSL证书过期时间【原理扫描】
详细描述	SSL 证书 就是遵守 SSL协议，由受信任的数字证书颁发机构CA，在验证服务器身份后颁发，具有服务器身份验证和数据传输加密功能。 备注：目前支持一个IP跟域名一一对应的使用场景
解决办法	仅用作信息收集，无需修复
威胁分值	3.3
危险插件	否
发现日期	2022-05-02

漏洞名称	获取SSL 证书中的hostname【原理扫描】
详细描述	SSL证书是用于建立安全连接的数字证书，它使得数据在用户的计算机和服务器之间加密传输成为可能。SSL证书由几个主要部分组成，包括：公钥，私钥，证书颁发机构，证书主题，有效期等。 通过SSL证书可以获取到目标使用的hostname。

解决办法	解决方案： 无需修复，仅仅为信息获取
威胁分值	3.5
危险插件	否
发现日期	2024-03-05

漏洞名称	检测到目标主机加密通信支持的SSL加密算法【原理扫描】
详细描述	该插件连接到目标主机服务，检测到目标服务加密通信使用的SSL加密算法。
解决办法	该漏洞仅仅是一个信息获取的漏洞，可以不做修复。
威胁分值	1.0
危险插件	否
发现日期	2001-01-01

漏洞名称	探测到服务器支持的SSL加密协议【原理扫描】
详细描述	为了保护敏感数据在传送过程中的安全，全球许多知名企业采用SSL（Security Socket Layer）加密机制。 SSL是Netscape公司所提出的安全保密协议
解决办法	该漏洞仅仅是一个信息获取的漏洞，可以不做修复。
威胁分值	0.0
危险插件	否
发现日期	1999-09-01

漏洞名称	Oracle MySQL 安全漏洞(CVE-2023-21963)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL 5.7.40 版本及之前版本和 8.0.31 版本及之前版本的 Server: Connection Handling 组件存在安全漏洞。高权限攻击者利用该漏洞可以通过多种协议访问网络来破坏 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuapr2023.html
威胁分值	2.7
危险插件	否
发现日期	2023-04-18
CVE编号	CVE-2023-21963
CNNVD编号	CNNVD-202304-1494
CNCVE编号	CNCVE-202321963
CNVD编号	CNVD-2023-67093

漏洞名称	Oracle MySQL curl/libcURL 安全漏洞(CVE-2023-38546)
详细描述	Oracle MySQL是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。Oracle MySQL Server 5.7.43及之前版本，8.0.34及之前版本和8.1.0存在安全漏洞，该漏洞源于MySQL Server中的Server: Compiling (curl)组件允许高权限攻击者通过多种协议进行网络访问来危害 MySQL 服务器。
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： https://www.oracle.com/security-alerts/cpuoct2023.html

威胁分值	3.7
危险插件	否
发现日期	2023-10-17
CVE编号	CVE-2023-38546
CNNVD编号	CNNVD-202310-916
CNCVE编号	CNCVE-202338546

漏洞名称	可以获取到MySQL/MariaDB/Percona/TiDB Server版本信息
详细描述	远程MySQL/MariaDB/Percona Server的版本信息可以获取。这允许攻击者根据版本信息来进行相应的攻击。您应当尽可能的改变或者隐藏这些信息。
解决办法	该漏洞仅是为了信息获取，建议隐藏敏感信息。
威胁分值	0.0
危险插件	否
发现日期	2001-01-01

漏洞名称	远程MySQL/MariaDB/Percona/TiDB Server版本泄露
详细描述	远程MySQL/MariaDB/Percona Server的版本信息可以获取。这允许攻击者根据版本信息来进行相应的攻击。您应当尽可能的改变或者隐藏这些信息。
解决办法	
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
8888,8000,80,8093	tcp	http	open
443	tcp	https	open
22	tcp	ssh	open
8082,8095,8098	tcp	www	open
3306	tcp	MySQL	open

3.2 安装软件信息

软件名称	版本号
WWW	nginx
Tomcat	9.0.65
nginx	1.25.2
OpenSSH	8.6
SSH	SSH-2.0-OpenSSH_8.6
Apache Tomcat	9.0.65

SSH Server	SSH-2.0-OpenSSH_8.6
MySQL	MySQL/5.7.39-log

3.3 操作系统类型

操作系统名字	版本号
Linux	3.10 - 4.11

3.4 端口Banner

端口	Banner
8095	nginx/1.25.2
8888	nginx
8082	Apache Tomcat/9.0.65
443	nginx
22	OpenSSH/8.6
8098	nginx/1.25.2
8093	nginx/1.25.2
8000	nginx/1.25.2
3306	MySQL/5.7.39-log
80	nginx
8082	Tomcat/9.0.65
3306	MySQL Server MySQL/5.7.39-log
22	SSH-2.0-OpenSSH_8.6

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 <= 漏洞风险值 <=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 <= 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 <= 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 <= 主机风险值 <= 10.0
比较危险	5.0 <= 主机风险值 < 7.0
比较安全	2.0 <= 主机风险值 < 5.0

非常安全	0.0 <= 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。