绿盟科技"网络安全漏洞扫描系统"
安全评估报告-主机报表

报表生成时间　2024-09-04 13:43:17

绿盟科技"网络安全漏洞扫描系统"安全评估报告-主机报表

目录

1 主机概况

主机风险	比较危险(5.1 分)
IP 地址	2.22.195.139
操作系统	linux:linux_kernel
系统版本	V6.0R04F04
插件版本	V6.0R02F01.3501
扫描起始时间	2024-09-04 10:44:50
扫描结束时间	2024-09-04 10:51:56
资产所属组织	未分组
漏洞扫描检查模板	自动匹配扫描
漏洞风险评估分	5.1 分
主机风险评估分	5.1 分

2 漏洞信息

2.1 漏洞概况

远程扫描

端口	协议	服务	漏洞
--	UDP	--	允许 Traceroute 探测
22	TCP	ssh	SSH 版本信息可被获取 探测到 SSH 服务器支持的算法
1935	TCP	http	可通过 HTTP 获取远端 WWW 服务信息
3306	TCP	mysql	猜测出远程 MySQL 数据库服务存在可登录的用户名口令 MySQL/MariaDB Server 用户存在弱口令 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
8080	TCP	http	可通过 HTTP 获取远端 WWW 服务信息

8991	TCP	http	可通过 HTTP 获取远端 WWW 服务信息
9000	TCP	http	可通过 HTTP 获取远端 WWW 服务信息
9001	TCP	http	Swagger API 未授权访问漏洞【原理扫描】 可通过 HTTP 获取远端 WWW 服务信息
9090	TCP	http	可通过 HTTP 获取远端 WWW 服务信息 远端 WEB 服务器上存在/robots.txt 文件
54321	TCP	postgresql	PostgreSQL Server 版本获取漏洞

2.2 漏洞详情

漏洞名称	猜测出远程 MySQL 数据库服务存在可登录的用户名口令
详细描述	本次扫描通过暴力猜测方式证实目标主机上的 MySQL 数据库服务存在可猜测的口令。 远程攻击者可通过猜测出的用户名口令对目标主机实施进一步的攻击，这将极大地威胁目标主机以及目标网络的安全。
解决办法	NSFOCUS 建议您采取以下措施以降低威胁: * 修改用户口令:设置足够强度的口令。 * 经常查看 MySQL 的漏洞情况,及时安装其更新升级包
威胁分值	5.0
危险插件	否
发现日期	2001-01-01

漏洞名称	MySQL/MariaDB Server 用户存在弱口令
详细描述	远端 MySQL/MariaDB 某些用户名设置了弱口令,通过暴力猜测恶意攻击者可轻易获取这些用户的口令,从而完全控制 mySQL/MariaDB server.
解决办法	为这些用户设置足够强壮的口令.设置密码,可使用命令: > mysql -u root [password] mysql> UPDATE user SET Password=PASSWORD('[new_password]') WHERE user='vulnerable_user'; mysql> FLUSH PRIVILEGES;
威胁分值	5.0
危险插件	否

发现日期	2005-01-01

漏洞名称	Swagger API 未授权访问漏洞【原理扫描】
详细描述	Swagger 是一个规范和完整的框架，用于生成、描述、调用和可视化 RESTful 风格的 We 服务。总体目标是使客户端和文件系统作为服务器以同样的速度来更新。相关的方法，参数和模型紧密集成到服务器端的代码，允许 API 来始终保持同步。 Swagger 生成的 API 文档，是直接暴露在相关 web 路径下的。所有人均可以访问查看。通过这一点即可获取项目上所有的接口信息。那么结合实际业务，例如如果有文件读取相关的接口，可能存在任意文件下载，相关的业务访问可能存在未授权访问等。 参考链接： https://www.sec-in.com/article/476
解决办法	1. 在生产节点禁用 Swagger2 2. 结合 SpringSecurity/shiro 进行认证授权，将 Swagger-UI 的 URLs 加入到各自的认证和授权过滤链中，当用户访问 Swagger 对应的资源时，只有通过认证授权的用户才能进行访问。 3. 结合 nginx/Filter 对对应的接口端点进行访问控制。
威胁分值	5.0
危险插件	否
发现日期	2022-10-26

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	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	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

漏洞名称	远端 WEB 服务器上存在/robots.txt 文件
详细描述	一些 WEB 服务器通过设置/robots.txt 使得一些搜索引擎或者索引工具更方便有效地工作。但/robots.txt 中往往存在一些系统信息，可能使攻击者获得该系统的额外信息。
解决办法	NSFOCUS 建议您采取以下措施以降低威胁： * 如果您的 robots.txt 中包含敏感信息，删除该文件。
威胁分值	1.0
危险插件	否
发现日期	2000-01-01

漏洞名称	PostgreSQL Server 版本获取漏洞
详细描述	可以获取到 PostgreSQL Server 版本
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	2018-05-16

3 其他信息

3.1 操作系统类型

操作系统名字	版本号
linux:linux_kernel	

3.2 端口 Banner

端口	Banner
54321	PostgreSQL DB
8991	nginx/1.25.3
1935	nginx/1.25.3
22	OpenSSH/8.9p1 Ubuntu 3ubuntu0.5
8080	nginx/1.25.3
3306	MySQL/5.7.44
9000	MinIO
9090	MinIO Console
3306	MySQL Server 5.7.44
22	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.5

3.3 远程端口信息

端口	协议	服务	状态
22	tcp	ssh	open
1935	tcp	http	open
8080	tcp	http	open
8991	tcp	http	open
9000-9001	tcp	http	open
9090	tcp	http	open
3306	tcp	MySQL	open
10050	tcp	zabbix-agent	open
54321	tcp	postgresql	open

3.4 安装软件信息

软件名称	版本号
PostgreSQL DB	
WWW	nginx
HTTP	1.1 302
MinIO	
nginx	1.25.3
OpenSSH	8.9p1 Ubuntu 3ubuntu0.5
MinIO Console	
SSH	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.5
SSH Server	SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.5
MySQL	5.7.44

3.5 应用程序信息

用户名	口令	应用
root	1****6	MySQL

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：

1. 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. 按照网络安全漏洞扫描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。