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　2025-04-17 09:01:46

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	非常危险(7.1 分)
IP 地址	172.18.3.195
操作系统	kylin_linux_advanced_server_v10_(halberd) V10
系统版本	V6.0R04F04SP05
插件版本	V6.0R02F01.3913
配置核查模板版本	V6.0R04F01.0000
扫描起始时间	2025-04-17 08:18:00
扫描结束时间	2025-04-17 08:26:34
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	7.1 分
主机风险评估分	7.1 分

2 漏洞信息

2.1 漏洞概况

远程扫描

端口	协议	服务	漏洞
--	ICMP	--	ICMP timestamp 请求响应漏洞
--	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
80	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
443	TCP	https	可通过 HTTP(S)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】 TLS 1.0 版协议检测【原理扫描】

			TLS 1.2 版协议检测【原理扫描】 TLS 1.3 版协议检测【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】
4118	TCP	netscript	TLS 1.0 版协议检测【原理扫描】 TLS 1.2 版协议检测【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】
5672	TCP	amqp	RabbitMQ 版本识别漏洞
6379	TCP	redis	Redis 资源管理错误漏洞(CVE-2024-46981) Redis 未授权访问漏洞(CNNVD-201511-230)【原理扫描】 Redis 输入验证错误漏洞(CVE-2024-51741)
8088	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息 远端 WEB 服务器上存在/robots.txt 文件 Jenkins 服务检测
8500	TCP	http	Consul 未授权访问漏洞【原理扫描】 可通过 HTTP(S)获取远端 WWW 服务信息 远端 WEB 服务器上存在/robots.txt 文件
9090	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10000	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10100	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10200	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10300	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息

10400	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10500	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10600	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10700	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10800	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
10900	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
11000	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息
15672	TCP	http	可通过 HTTP(S)获取远端 WWW 服务信息

2.2 漏洞详情

漏洞名称	Redis 资源管理错误漏洞(CVE-2024-46981)
详细描述	Redis 是美国 Redis 公司的一套开源的使用 ANSI C 编写、支持网络、可基于内存亦可持久化的日志型、键值（Key-Value）存储数据库，并提供多种语言的 API。 Redis 存在资源管理错误漏洞。攻击者利用该漏洞可以远程执行代码。
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://github.com/redis/redis/security/advisories/GHSA-39h2-x6c4-6w4c
威胁分值	7.0
危险插件	否
发现日期	2024-09-16
CVE 编号	CVE-2024-46981
CNNVD 编号	CNNVD-202501-529
CNCVE 编号	CNCVE-202446981

漏洞名称	Redis 未授权访问漏洞(CNNVD-201511-230)【原理扫描】
详细描述	redis 端口对外开放并且没有配置认证选项，未授权用户可直接获取数据库中所有信息，造成严重的信息泄露。
解决办法	方法一: 可以修改绑定的 IP、端口和指定访问者 IP 具体根据实际情况来设定，也可以直接在服务器防火墙上做设置。 方法二:

	设置访问密码 在 redis.conf 中找到“requirepass”字段，取消注释并在后面填上你需要的密码。 注：修改 redis 的配置需要重启 redis 才能生效。
威胁分值	6.0
危险插件	否
发现日期	2015-03-26
CNNVD 编号	CNNVD-201511-230
CNVD 编号	CNVD-2019-21763

漏洞名称	Redis 输入验证错误漏洞(CVE-2024-51741)
详细描述	Redis 是美国 Redis 公司的一套开源的使用 ANSI C 编写、支持网络、可基于内存亦可持久化的日志型、键值（Key-Value）存储数据库，并提供多种语言的 API。 Redis 7.0.0 版本及之后版本存在输入验证错误漏洞。攻击者利用该漏洞可以创建格式错误的 ACL 选择器，访问该选择器时会触发服务器崩溃并随后导致拒绝服务。
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://github.com/redis/redis/security/advisories/GHSA-prpq-rh5h-46g9
威胁分值	4.4
危险插件	否
发现日期	2024-10-31
CVE 编号	CVE-2024-51741
CNNVD 编号	CNNVD-202501-534
CNCVE 编号	CNCVE-202451741

漏洞名称	Consul 未授权访问漏洞【原理扫描】
详细描述	Consul 是 HashiCorp 公司推出的一款开源工具，用于实现分布式系统的服务发现与配置。与其他分布式服务注册与发现的方案相比，Consul 提供的方案更为“一站式”。Consul 内置了服务注册与发现框架、分布一致性协议实现、健康检查、Key/Value 存储、多数据中心方案，不再需要依赖其他工具（例如 ZooKeeper 等），使用方式也相对简单。 Consul 默认配置下缺少访问控制，导致攻击者可以获取敏感信息
解决办法	请增加 Consul 的授权管理控制
威胁分值	6.5
危险插件	否
发现日期	2021-08-07

漏洞名称	ICMP timestamp 请求响应漏洞
详细描述	远程主机会回复 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	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	1999-06-07
CVE 编号	CVE-1999-0524
CNNVD 编号	CNNVD-199708-003
CNCVE 编号	CNCVE-19990524
CVSS 评分	2.1

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，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	1999-06-07
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(S)获取远端 WWW 服务信息
详细描述	本插件检测远端 HTTP(S) 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	TLS 1.0 版协议检测【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。 远程服务利用旧版 TLS 加密流量。
解决办法	启用 TLS 1.2 和/或 1.3 支持，禁用 TLS 1.0 支持。
威胁分值	1.0
危险插件	否
发现日期	2001-01-01

漏洞名称	TLS 1.2 版协议检测【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。 远程服务接受使用 TLS 1.2 加密的连接
解决办法	协议探测，无需修复
威胁分值	1.0
危险插件	否
发现日期	2001-01-01

漏洞名称	TLS 1.3 版协议检测【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。 远程服务接受使用 TLS 1.3 加密的连接
解决办法	协议探测，无需修复
威胁分值	1.0
危险插件	否
发现日期	2001-01-01

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	RabbitMQ 版本识别漏洞
详细描述	可以识别到 RabbitMQ 的版本信息。
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	2021-03-01

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	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	Jenkins 服务检测
详细描述	Jenkins 之前叫做 Hudson，是 Jenkins CI 社区基于 Java 开发的一种持续集成工具，用于监控秩序重复的工作。 远程主机运行着 Jenkins。
解决办法	修复建议：可以不修复或者卸载 Jenkins。
威胁分值	0.0
危险插件	否
发现日期	2013-11-07

3 配置合规信息

4 状态合规信息

5 其他信息

5.1 操作系统类型

操作系统名字	版本号
kylin_linux_advanced_server_v10_(halberd) V10	

5.2 端口 Banner

端口	Banner
443	OpenResty web app server/1.27.1.1
27017	MongoDB
8500	HashiCorp Consul/1.15.4
80	OpenResty web app server/1.27.1.1
1433	Microsoft SQL Server
8088	Jetty/12.0.14
22	OpenSSH/8.2
15672	jquery.js/3.5.1
15672	Cowboy httpd
6379	Redis key-value store/7.4.1
11000	Kestrel
443	openresty/1.27.1.1
80	openresty/1.27.1.1
10000	Kestrel
10100	Kestrel
10500	Kestrel
10400	Kestrel
8088	Jetty(12.0.14)
10700	Kestrel
10600	Kestrel
10300	Kestrel
10800	Kestrel
10200	Kestrel
10900	Kestrel
22	SSH-2.0-OpenSSH_8.2

5.3 远程端口信息

端口	协议	服务	状态
22	tcp	ssh	open
443	tcp	https	open
1433	tcp	ms-sql-s	open
4118	tcp	netscript	open
80	tcp	http	open
8088	tcp	http	open
8500	tcp	http	open
9090	tcp	http	open
10000	tcp	http	open
10100	tcp	http	open

10200	tcp	http	open
10300	tcp	http	open
10400	tcp	http	open
10500	tcp	http	open
10600	tcp	http	open
10700	tcp	http	open
10800	tcp	http	open
10900	tcp	http	open
11000	tcp	http	open
15672	tcp	http	open
50000	tcp	http	open
5672	tcp	amqp	open
6379	tcp	redis	open
27017	tcp	mongodb	open

5.4 安装软件信息

软件名称	版本号
jquery.js	3.5.1
Cowboy httpd	
WWW	Kestrel;
HTTP	1.0 200 OK
Kestrel	
OpenSSH	8.2
Redis	redis
Jetty	12.0.14
RabbitMQ	Rabbit
HashiCorp Consul	1.15.4
OpenResty web app server	1.27.1.1
openresty	1.27.1.1
MongoDB	
Redis key-value store	7.4.1
Jetty(12.0.14)	
Microsoft SQL Server	
SSH	SSH-2.0-OpenSSH_8.2
SSH Server	SSH-2.0-OpenSSH_8.2

6 参考标准

6.1 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。

6.2 单一配置检查项等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <=检查项风险值<= 10	不当的配置导致攻击者可以通过其他方式获得管理员权限、或者只有管理员权限才能加固的配置。
中	4 <=检查项风险值< 7	不当的配置导致攻击者可以对主机进行破坏或者收集主机的信息、或者遭受攻击后，重要事件没有记录。
低	0 <=检查项风险值< 4	不当地配置对主机安全不会造成太大的影响。

6.3 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。