

主机安全

实践教程





【版权声明】

©2013-2025 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云 事先明确书面许可,任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成 对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

# 🔗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的 商标,依法由权利人所有。未经腾讯云及有关权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复 制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人商标权的侵犯,腾讯云将依法采取措施追究法律责 任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则, 腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或 95716。



# 文档目录

实践教程

主机安全等保测评解读 漏洞自动修复 扫码安全登录 恶意文件处理

# 实践教程 主机安全等保测评解读

最近更新时间: 2024-11-14 10:58:12

# 等保标准解读

腾讯主机安全(Cloud Workload Protection,CWP)产品符合等级保护2.0标准体系主要标准。根据《网络 安全等级保护基本要求》(GB/T 22239-2019),腾讯主机安全(仅限专业版、旗舰版且已购买日志分析)满足 第三级及以下安全要求:

序号	等保标准章节	等保标准序 号	等保标准内容	对应功能描述
1	安全区域边界—边 界防护	8.1.3.1 c)	应能够对内部用户非授权联 到外部网络的行为进行检查 和限制。	主机安全支持对云服务器 非授权恶意外联到外部恶 意域名,IP 地址的行为进 行检测和拦截。
2	安全区域边界—入 侵防范	8.1.3.3 a)	应在关键网络节点处检测、 防止或限制从外部发起的网 络攻击行为。	主机安全支持检测和阻断 暴破攻击,并能对常见的 网络攻击进行检测,部分 漏洞支持一键漏洞防御。
3	安全区域边界—入 侵防范	8.1.3.3 b)	应在关键网络节点处检测、 防止或限制从内部发起的网 络攻击行为。	主机安全可检测云服务器 系统层和应用层的主动外 联和攻击行为,对进程, 命令异常行为进行告警。
4	安全区域边界一入 侵防范	8.1.3.3 c)	应采取技术措施对网络行为 进行分析,实现对网络攻击 特别是新型网络攻击行为的 分析。	主机安全支持基于主机、 网络、云平台的安全数据 进行分析,实现对挖矿、 勒索、木马、蠕虫等新型 攻击进行检测告警。
5	安全区域边界—入 侵防范	8.1.3.3 d)	当检测到攻击行为时,记录 攻击源 IP、攻击类型、攻击 目的、攻击时间,在发生严 重入侵事件时应提供报警。	主机安全在检测到暴破攻 击时,会记录来源 IP、来 源地、被攻击服务器 IP/名 称、端口、协议、用户 名、时间、破解状态、阻 断状态并进行告警。
6	安全区域边界一安 全审计	8.1.3.5 b)	审计记录应包括事件的日期 和时间、用户、事件类型、	主机安全支持服务器登录 审计,记录信息包括来源



			事件是否成功及其他与审计 相关的信息。	IP、来源地、服务器 IP/名 称、登录用户名、登录时 间、状态、危险等级。
7	安全计算环境一身 份鉴别	8.1.4.1 a)	应对登录的用户进行身份标 识和鉴别,身份标识具有唯 一性,身份鉴别信息具有复 杂度要求并定期更换。	主机安全基线检查能力支 持对云服务客户登录配置 和密码复杂度进行定期安 全检查,对风险项进行预 警并提供安全建议。
8	安全计算环境一身 份鉴别	8.1.4.1 b)	应启用登录失败处理功能, 应配置并启用结束会话、限 制非法登录次数和当登录连 接超时自动退出等相关措 施。	主机安全支持主机登录失 败防御配置,可灵活设定 在一定时间段内多次登录 失败后锁定用户的规则。
9	安全计算环境一身 份鉴别	8.1.4.1 c)	当进行远程管理时,应采取 必要措施防止鉴别信息在网 络传输过程中被窃听。	主机安全支持对远程管理 的不当配置进行检查,如 有禁止使用 telnet 基线检 查。
1 0	安全计算环境—访 问控制	8.1.4.2 b)	应重命名或删除默认账户, 修改默认账户的默认口令。	主机安全支持对账户权限 配置检查,资产管理支持 展示所有可登录账号,支 持默认弱口令安全检查, 发现风险时进行告警并提 供修复建议。
1 1	安全计算环境一访 问控制	8.1.4.2 c)	应及时删除或停用多余的、 过期的账户,避免共享账户 的存在。	主机安全支持对云服务器 账户进行安全配置检查, 资产管理支持展示所有登 录账号,支持账户登录 IP 异常时进行告警,避免共 享账户存在。
1 2	安全计算环境 <del>一</del> 安 全审计	8.1.4.3 a)	应启用安全审计功能,审计 覆盖到每个用户,对重要的 用户行为和重要安全事件进 行审计。	主机安全支持对云服务器 账户登录操作进行记录, 以及高危命令、高危操作 的审计。
1 3	安全计算环境—安 全审计	8.1.4.3 b)	审计记录应包括事件的日期 和时间、用户、事件类型、 事件是否成功及其他与审计 相关的信息。	主机安全日志记录包括主 机 IP、主机实例 ID、账 户、源 IP、目的 IP、进程 ID 端口、事件类型、发生 时间、动作策略等内容。

1 4	安全计算环境 <del>一</del> 安 全审计	8.1.4.3 c)	应对审计记录进行保护,定 期备份,避免受到未预期的 删除、修改或覆盖等。	主机安全产品支持日志审 计存储功能,可存储至少6 个月内的日志数据,不同 租户使用完全独立的日志 空间,日志数据有多副本 备份机制。
1 5	安全计算环境一入 侵防范	8.1.4.4 b)	应关闭不需要的系统服务、 默认共享和高危端口。	主机安全资产管理支持对 云服务器上运行的服务、 进程、开放的端口进行统 一管控。
1 6	安全计算环境一入 侵防范	8.1.4.4 c)	应通过设定终端接入方式或 网络地址范围对通过网络进 行管理的管理终端进行限 制。	主机安全支持添加主机登 录 IP 地址白名单,非白名 单内用户登录将被拦截。 配合安全组实现云上网络 管理和限制。
1 7	安全计算环境一入 侵防范	8.1.4.4 e)	应能发现可能存在的已知漏 洞,并在经过充分测试评估 后,及时修补漏洞。	主机安全支持检测 Linux 软件漏洞、Windows 系 统漏洞、Web-CMS、应 用漏洞、应急漏洞,评估 风险级别并提供修复建 议。
1 8	安全计算环境一入 侵防范	8.1.4.4 f)	应能够检测到对重要节点进 行入侵的行为,并在发生严 重入侵事件时提供报警。	主机安全支持检测重要节 点的入侵行为,主要包括 恶意文件,异常登录,密 码破解,恶意请求,高危 命令,反弹 shell,本地提 权,文件篡改等,提供告 警及部分主动阻断能力。
1 9	安全计算环境 <del>一</del> 恶 意代码防范	8.1.4.5	应采用免受恶意代码攻击的 技术措施或采用主动免疫可 信验证机制及时识别入侵和 病毒行为,并将其有效阻 断。	主机安全支持恶意文件查 杀,实时监测木马,病 毒,并自动隔离。
2 0	安全管理中心一安 全管理	8.1.5.3 a)	应对安全管理员进行身份鉴 别,只允许其通过特定的命 令或操作界面进行安全管理 操作,并对这些操作进行审 计。	主机安全支持通过控制台 对云资源进行安全管理操 作,能对登录行为、高危 命令进行审计。

🔗 腾讯云

2 1	安全管理中心一安 全管理	8.1.5.3 b)	应通过安全管理员对系统中 的安全策略进行配置,包括 安全参数的设置,主体、客 体进行统一安全标记,对主 体进行授权,配置可信验证 策略等。	主机安全支持通过控制台 对系统中的安全策略进行 配置。
2 2	安全管理中心一集 中管控	8.1.5.3 e)	应对安全策略、恶意代码、 补丁升级等安全相关事项进 行集中管理。	主机安全支持漏洞集中管 理,恶意代码检测和隔 离。

# 等保合规基线策略

腾讯云主机安全默认提供 等保合规基线策略,支持对基线检测项的定期检测和一键检测,帮助了解基线通过率及风 险情况,提供基线和检测项的风险等级和修复建议,有助于您快速整改,满足等保合规要求。以下为等保合规支持检 测项:

基线分类	基线名称	包含的检查项数量
基33万尖     基3       等     等       等     等       等保二级     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等       等     等	等保二级-CentOS 6安全基线检查	16
	等保二级-CentOS 7安全基线检查	18
	等保二级-CentOS 8安全基线检查	16
	等保二级Ubuntu 14安全基线检查	19
	等保二级Ubuntu 16安全基线检查	19
	等保二级Ubuntu 18安全基线检查	21
	等保二级Ubuntu 20安全基线检查	29
等保三级	等保三级-CentOS 6安全基线检查	27
	等保三级-CentOS 7安全基线检查	31
等保三级	等保三级-CentOS 8安全基线检查	36
	等保三级Ubuntu 14安全基线检查	35
	等保三级Ubuntu 16安全基线检查	33
	等保三级Ubuntu 18安全基线检查	40
	等保三级Ubuntu 20安全基线检查	48



等保三级-Windows 2008安全基线检查	19
等保三级-Windows 2012安全基线检查	19
等保三级-Windows 2016安全基线检查	19

腾讯云

# 漏洞自动修复

最近更新时间: 2025-04-03 15:58:32

#### 本文将为您介绍自动修复漏洞的实践教程。

#### ▲ 注意:

自动修复漏洞可能会在您的主机上执行命令,可能影响到正在运行的应用或系统核心组件,可能影响您业务 的连续性。对于核心业务主机,建议您充分考虑后再决策修复哪些漏洞及漏洞修复的先后顺序。

## 限制说明

- 支持修复的主机: 仅支持腾讯云上的 CVM 服务器(主机安全客户端在线,且已绑定主机安全旗舰版授权)。
- 支持自动修复的漏洞:Linux 软件漏洞(部分)、Web-CMS 漏洞(部分)。

# 操作指南

- 1. 登录 主机安全控制台,单击左侧导航中的漏洞管理,底部可见漏洞检出列表。
- 在漏洞列表中,分为应急漏洞、全部漏洞两类,由于均是从检出维度展示漏洞,功能差异不大,下面以全部漏洞 作为示例,说明漏洞自动修复各个步骤。

#### ! 说明:

- 漏洞修复优先级: 应急漏洞 > 高优修复漏洞 > 全部漏洞。
- 可自动修复的漏洞在操作列中有自动修复操作,暂不可自动修复的漏洞在操作列中有修复方案操作。

应急漏洞 全部漏洞											◎ 显示统计图表
自动游复 更多操作 v 全部漏洞标签 v	全部威胁等级 * 待修复	• <b>(</b>	展示高优修复漏洞 判定规则							请输入混洞	名称/CVE編号搜索 Q 🗘 🌣 🛓
漏洞名称标签	检测方式 🔻	漏洞类型 ▼	威胁等级	全网攻击热度 下	CVSS	CVE编号	最后扫描时间 \$	影响主机 \$	处理状态	是否支持自动修复 <b>T</b>	操作
-			中危		6.8		2025-04-01 10:22:15	1	🕡 待修复	<ul> <li>可自动修复</li> </ul>	修覽方案   更多 🔻
			严重		9.8		2025-04-01 10:22:15	1	♥ 待修复	•可自动修复	修复方案   更多 ▼
			高能		7.5		2025-04-01 10:22:15	t	17 待修复	•可自动修复	修复方案   更多 ▼
			高能		8.2		2025-04-01 10:22:15	1	♥ 待修复	•可自动修复	修复方案   更多 ▼
100			高危		7.6		2025-04-01 10:22:15	t	17 待修复	•可自动修复	修复方案   更多 ▼
			高度		7.5	10.007	2025-04-01 10:22:15	t	⑦ 待修复	•可自动修复	修复方案   更多 ▼
		100	高危	***	8.2	1.000	2025-04-01 10:22:15	t	()待修复	<ul> <li>可自动修复</li> </ul>	修复方案   更多 ▼

## 步骤1: 查看漏洞详情

单击**自动修复**,打开漏洞详情弹窗。



#### PostgreSQL JDBC远程代码执行漏洞(CVE-2022-21724) CVSS评分 9.8 × 漏洞详情 👤 导出 攻击路径 (AV) 漏洞名称 PostgreSQL JDBC远程代码执行漏洞(CVE-2022-21724) 可用性影响 (A) 攻击难度 (AC) 漏洞标签 远程利用 漏洞类型 应用漏洞 完整性影响(1) 权限要求 (PR) 威胁等级 严重 CVE编号 CVE-2022-21724 披露时间 2022-02-02 机密性影响 (C) 用户交互 (UI) 影响范围 (S) 漏洞描述 PostgreSQL JDBC Driver是一个用 Pure Java (Type 4) 编写的开源 JDBC 驱动程序, 用于 PostgreSQL 本地网络协议中进行通信。 PostgreSQL JDBC Driver (简称 PgJDBC)存在安全漏洞,该漏洞源于pgjdbc连接属性 提供的类名实例化插件实例,驱动程序在实例化类之前并不验证类是否实现了预期的接 口从而导致远程代码。 修复方案 修复方案 建议受影响的用户及时更新pgjdbc到安全版本; 42.2.x及之前版本,请升级到42.2.25或42.3.2及以上版本; 42.3.x用户请升级到42.3.2及以上版本; 下载链接: https://jdbc.postgresql.org/download/ 扫描到服务器存在漏洞风险,建议立即对相关主机进行快照备份,避免遭受损失。 参考链接 https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-v7wg-cpwc-24m4 https://github.com/pgjdbc/pgjdbc/commit/f4d0ed69c0b3aae8531d83d6af4c57f22312c813 https://security.netapp.com/advisory/ntap-20220311-0005/ 更多2条参考连接

#### 影响主机范围 (1)

修复	重新扫描	忽略	待修复	~		请选择资源属性后输入关	键字进行过滤(仅支持	寺単个値) 🔍 🗘 🛓
主机名称	尔实 IP地址		防护版本 ▼	服务器状态 ▼	扫描时间	说明	状态	操作
	公 Эт 17 内		₩ 旗舰版	运行中	首次: 20 最近: 20	/v. Г		重新扫描 忽略漏洞

# 步骤2:选择需要修复的主机

1. 在受影响的服务器列表中选择您要修复的主机,单击**修复**。



影响主机范围 (10) 影响组件范围	(4)					
修复重新扫描 忽略	全部	•		请选择资源属性后输入关键字	进行过濾(仅支持	単个値) Q 🖞 🛓
主机名称/实 IP地址	防护版本 ▼	服务器状态 ▼	扫描时间	说明	状态	操作
▲ 公本 ● 単元标金	🍲 旗舰版	运行中	首次: 21 最近: 21	2 ⊈ 9 Г <u>⊓</u>	⊖ 待修复	修复 重新扫描 忽略漏洞
✓ 3 公	₩ 旗舰版	运行中	首次: 2 最近: 2	3 软 3 匠	⊖ 待修复	修复 重新扫描 忽略漏洞

2. 在确认修复弹窗中,单击确定,进入修复漏洞页面。

## 步骤3:选择是否创建快照

- 1. 在修改漏洞页面,确认修复主机范围,单击下一步。
- 2. 根据实际需求选择修复方式:
  - 自动创建快照并修复:支持设置快照名称、快照保存时长(3天、7天、15天,建议保留7天时间,以便在有 需求的情况下及时回滚)。
  - 不创建快照直接修复: 若今日所选修复主机均已创建过快照,此选项将变为可选状态。

← 修复漏洞	: Git 代码执行漏洞(CVE-20	23-29007)		* 关闭	甜抽屉后点击"修复详情"按钮方可再次查看流程 🗙
	✔ 修复说明	$\rightarrow$	2 选择修复方式		③ 创建快照&修复漏洞
<ol> <li>漏洞的</li> <li>修复</li> <li>此漏</li> <li>主机</li> <li>请参</li> </ol>	多复说明 可能持续10~20分钟,具体时长与服务 洞执行修复后需重启方可修复成功,强 进行漏洞补丁修复行为可能存在一定风 考 <b>主机漏洞修复指南 Ľ</b>	器当前工作情况相关, 议您根据业务情况谨慎 N险,为了防止出现业务	请耐心等待; 选择修复时间; ;中断或异常,建议您先通过 控	制台手动创建快照并自	目行搭建环境充分测试修复方案,具体操作
○ 自动创建快照	群修复 不创建快照	直接修复			
快照名称	漏洞修复_Git 代码执行漏洞(CVE-	2023-29007)		<b>()</b>	
快照保存时长	7天 (建议)			•	
	1. 创建快照建议保留7天时间,以便 2. 创建快照需要额外的费用(500G	在有需求的情况下及时 B/天约2元) ,详细计慧	回滚。 阿见 <b>快照价格总览 [2</b>		

# 步骤4:开始修复

单击**确认修复**开始修复漏洞,您可查看当前修复的情况。

← 修复漏洞: Git 代码执行漏洞(CVE-2023-29007)

\* 关闭抽屉后点击"修复详情"按钮方可再次查看流程 🗙

	✔ 修复说明	✔ 选择修	复方式	3 创建快照&修复漏洞		
	全部修築	夏成功		已修复主机/目标主机 开始时间 结束时间	2023-06-0 2023-06-0	<mark>2 / 2</mark> 09 15:43:09 09 15:44:47
⊘ 创建	皇快照					▼收起
服	务器IP/名称	快照名称	创建状态		快照创建时间	
1 <sup>.</sup> w	)	漏洞修复_Git 代码执行漏洞(CVE-202	⊘ 创建成功		2023-06-09 15:43:47	
1	境	漏洞修复_Git 代码执行漏洞(CVE-202	⊘ 创建成功		2023-06-09 15:43:57	
⊘ 修复	复漏洞: Git 代码执行漏洞(CVE-202	23-29007)				▼收起
BR	务器IP/名称	修复状态		修复时间		
1		20动) 🥥 修复成功		2023-06-09 1	5:44:33	
1		⊘ 修复成功		2023-06-09 1	5:44:47	
◎ 修言	百全成					

# 步骤5: 查看主机状态变更

返回**漏洞详情**,关注主机状态变更。若漏洞修复失败,状态则为修复失败;若漏洞修复成功,状态则变更为已修复。



# Git 代码执行漏洞(CVE-2023-29007) CVSS联分 7.8 X 漏滴述 Git 是一套免费,开源的分布式版本控制系统。Git存在注入漏洞。攻击者利用该漏洞可以送程执行代码。 影响范围 (S) · 《 使复方案 · 》 修复方案 修复方案 · 提议您更新当前系统或软件至最新版,完成漏洞的修复。 · 日插到服务器存在漏洞风险,建议立即对相关主机进行快服备份,避免遭受损失。 · 参考链接 · https://github.com/git/git/blob/9ce9dea4e1c2419cca126d29fa7730baa078a11b/Documentation/RelNotes/2.30.9.bt/ · 更多名参考连接

影响主机范围 (10) 影响组件范围 (4)									
修复重	新扫描	忽略 全部			请选择资源属性后输入关键字进行过滤(仅支持单个值)		寺単个値) Q	¢	Ŧ
主机名称/实	. IP地址	防护版本 🔻	服务器状态 ▼	扫描时间	说明	状态	操作		
「「「「」」	公 内	5 / 旗舰版	运行中	首次: 2023-05- 最近: 2023-06-	-23 17:42:42 -09 15:44:47	⊘ 已修复	回滚 重新扫描 修复详情	ŧ	
	公 内	🍲 旗舰版	运行中	首次: 2023-05- 最近: 2023-06-	-16 01:39:23 -09 15:44:32	⊘ 已修复	回滚 重新扫描 修复详情	ŧ	

- 漏洞修复后,若对您的业务产生了较大影响,您可单击回滚操作,将引导前往 云服务器 > 快照列表,选择您修复前创建的快照进行回滚。回滚成功后,请重启服务器,对漏洞进行重新扫描。
- 漏洞修复后,可进行重新扫描操作,再次验证漏洞是否已修复。
- 漏洞修复后,也可单击修复详情操作,查看修复的具体过程。

# 🔗 腾讯云

# 扫码安全登录

最近更新时间: 2025-05-29 11:32:32

扫码安全登录功能允许用户仅通过微信扫码验证即可完成服务器登录,无需输入密码。该功能有效防止黑客的暴力破 解攻击,从而进一步提高服务器的安全性,同时也增加了登录的便利性。本文将向您介绍扫码安全登录的实践教程。

#### ▲ 注意:

- 启用扫码登录后,将用微信扫码验证腾讯云账号的方式替代密码登录,这可能会影响到相关自动化业务。同时,在使用 SSH 相关的协议时,虽然支持 SCP、SFTP、RSYNC、GIT、MOSH 等场景,但暂不支持基于 SSHFS 协议的文件夹挂载等场景。
- 对于核心业务的主机,建议您充分考虑后再决策是否更改登录方式。

## 限制说明

- 支持的主机类型: 仅限于腾讯云上的 CVM/Lighthouse 服务器(要求主机安全客户端在线)。
- 支持的登录用户: 机器所属的腾讯云子账号及其主账号,或经 CAM 授权的其他腾讯云账号。
- 支持 SSH 客户端: CMD、PowerShell、Putty、Xshell、终端、WeTERM、Termius 等。

## 步骤1: 配置登录方式

- 1. 登录 主机安全控制台,在左侧导航栏,单击**主机列表。**
- 2. 在主机列表中,右侧找到对应实例,在操作项中选择更多,单击开启扫码登录。

安装主机安全客户端 升级版本	全部服务器	▼ 全地域	T			请	选择资源属性	后输入	关键字搜索(仅支	持单个值)	Q ¢ ¢ ±
主机防护状态分类	主机名称/实例ID	IP地址	操作系统 ▼	地域/所属网络 🔻	风险	入侵检测	漏洞风险	基线	agent状态 ▼	防护版本	操作
全部主机										<b>兰</b> 重版	
风险主机									• 防护中	• (Lighth	卸载 更多 ▼
旗舰版主机											授权管理
专业版主机									• 未防护	•	开启扫码登录
基础版主机											
未安装客户端(无防护)									• 已离线 访	• 基础版	重新安装
已离线									• 已离线	• 旗舰版	上 重新安装 授权管理
已关机											
近15日新增									• 防护中	•基础版	卸载

3. 单击开启,开启后该服务器优先通过微信扫码登录腾讯云账号的方式登录。



## 确认开启 扫码安全登录 功能?

开启后,优先通过微信扫码登录腾讯云账号的方式登录轻量应用服务器,可在主机安全控制台/轻量应用服务器控制台进行关闭。开启过程需要3-5分钟。

#### 支持的ssh协议包括:

ssh相关协议中,支持协议scp、sftp、rsync、git、MOSH相关场景,暂无法支持基于SSHFS协议的挂载文件夹等场景,开启后5分钟内生效。

#### 支持的ssh客户端包括:

-Linux -MAC: 终端、WeTERM、Termius -Windows: CMD、PowerShell、Putty、Xshell

开启 取消

## 步骤2:终端发起登录

开启扫码登录后,SSH 命令行输入实例 IP 后弹出二维码,使用微信扫码将会进入腾讯云助手小程序进行身份认证,完成认证后即可完成登录。

#### 🕛 说明:

如果二维码显示有问题,请通过下方提供的 URL 在网页中打开二维码图片。



almainhan@ALMAINHAN-MB0 ~ % almainhan@ALMAINHAN-MB0 ~ % ssh root@11	
and the second	
**************************************	**************************************
Visit the URL: https://s	)g
***************************************	******

 扫码登录服务异常时将自动降级到常规的密码登录,并增加人机校验兜底策略,输入随机数完成认证后可通过密 码登录的方式完成登录。



# 步骤3:小程序验证

1. 扫码后打开腾讯云助手,选择登录方式登录腾讯云账号以完成校验。





2. 成功登录腾讯云账号,单击**确认登录**,校验该账号登录服务器的权限后,通过验证完成登录。





# 恶意文件处理

最近更新时间: 2025-04-29 10:58:42

当用户腾讯云账号下的服务器被检出存在恶意文件,主机安全若发现该文件没有命中文件白名单,则会触发实时告 警。

### 处理步骤

在收到恶意文件告警后,请按照下列步骤进行操作:

- 1. 登录 主机安全控制台,在左侧导航栏,选择入侵检测 > 文件查杀。
- 2. 在文件查杀页面,通过告警资产实例 ID 进行搜索,定位到具体告警并单击详情。

主机安全	文件查杀						☆ 查杀设置
- 安全概览	<b>告警列表</b> 白名单文件						
资产中心	<ol> <li>功能使用说明</li> </ol>						◎ 隐藏说明
── 资产概览	5	山机夫训诉/按翻版	文件查杀i	设置/下发手		() 生物从田	
🗄 主机列表	功能操作指引 文件者	1 <b>32 マ 32 nBX BARGINS</b> E杀检测属于专业版/旗舰版功能,请先	✓ 动扫描 → 社査条役置句:	场空时检测 空时营榨和自动	开启文件查杀告警,当检测到在	存在恶意文件或 可在告警列表中:	查看告警详情及建议方案,点
⋒ 资产指纹	Q <sup>升级月</sup> 功能介绍 <b>升级</b> 月	ī本。 <b>ī本</b>	「相當」 「「「」」 「「」」 「「」」 「「」」 「」」 「」」 「」」 「」」	动化病毒查杀,您也可以手动	异常进程时将及时向您告警。 <b>告警设置</b>	击"立即处理"可;	对告警进行处理操作。 
🕢 安全预警			文件查杀设置	一键扫描			
安全加固							
○ 漏洞管理	<b>风险概况</b> 病毒库更新日期:2024-10-22	00:00:05					近一次检测时间:2024-10-21 02:00:02 查看详情
(2) 至33官理 入侵防御	旗舰版   专业版   基础版	待处理恶意文件 <b>つ</b>	待处理异常进程	影响服务器			检测已开启(每3天02:00~06:00) ♪
○ 入侵检测 ^		<b>0</b> ↑	U↑	台		(O) 实的	监控已升启(硕准模式) 🖌
・ 文件査杀	平音文件 ① 日世洪程 ①						
・ 异常登录							
· 密码破解	<b>恶意文件自动隔离:</b> 防护模	式: 👽 标准模式 🛈 🗸					
・ 恶意请求	· 唐高   标记户外理   更	8办理 ▼			洗探时间 洗探时间	意の問い	0.04
・高危命令	主和名称/定例ID	IDimite 路谷		病壳之/松山己鹜	成功等码 ▼ 首次发现时间 ★		
・ 本地提校 ・ 反弾Shell		W AGAIL FRITE		Script Traign Exec. Jonny	00.07/93X ) EI/AA/91/97 V	ax 42 ta 00 € 1 € V	Zlabshua , DRIF
▽ 高级防御 ∨	in prime	内.	Ŧ		严重 2024-09-03 10:22:41	2024-10-21 02:18:46	
安全运营		公 · 内 ·		Suspicious.(aiScore=m)	严重 2024-09-03 10:22:56	2024-10-21 02:18:42	⊖待处理 ③ 详情 处理 ▼ □
□ 日志分析		11	Ť	<b>U</b>			
三 给产品打个分 🕥 🦷	a prime	公内	Ŧ	Linux.HackTool.Ish.Aplw	严重 2024-09-03 11:02:49	2024-10-21 02:18:32	

3. 查看告警详情后,请确认该恶意文件是否误报,若是误报,请执行步骤4,若不是误报,请执行步骤5。

#### 🕛 说明:

该恶意文件是否误报,可结合以下几种方式判定:

- 联系业务团队判断该文件是否是业务正常运行所需文件。
- 查询威胁情报,判断该文件是否被外网标记为恶意样本。
- 该文件行为是否导致进一步触发更多告警。

# 🔗 腾讯云

#### • 联系 安全专家服务。

4. 明确是误报,请将该文件加入白名单,后续再次检出此文件将被忽略,不会产生告警,并联系我们反馈误报。

添加白名单		×
白名单内容		
*加白方式	○ 文件MD5	
* 文件MD5	请输入文件MD5,多个回车换行,一行输入一个MD5 示例: 19a7ae0aea306b7165b3431c90f613b2 7cbfd6268396ad16e1880e6d3f2e2f2e	
告警处理	✔ 对符合本规则的历史"待处理"告警执行加白操作	
<b>生效主机范围(</b> 选择范围•	(已选择 3 台) ● 全部专业版和旗舰版服务器	

5. 明确不是误报,请参考告警详情中的修复建议进行处理。



恶意文件详	<b>情                                    </b>			×
隔离	标记已处理加入白名单忽略	删除记录		
告警详情	进程树 NEW 事件调查 NEW			
<b>风险主机</b> 主 案 2	机名称 ·例 ID 公 内	<ul> <li>首次发现时间</li> <li>最近检测时间</li> </ul>	2024-09-03 10:22:56 2024-10-21 02:18:42	
病毒文件				
Ì	病毒名	威胁等级 检出引擎 <b>《</b> 标签特征	严重 S Exploit	
E	文件名	文件大小 文件路径 文件 <b>MD5</b> 最近访问时间 最近修改时间	1.50 KB 2024-10-20 12:33:55 2024-09-03 10:22:39	
⑦ 危害描述	发现主机/容器上存在漏洞利用程序,您的主机/容错漏洞利用程序是指黑客针对某些特定的程序漏洞编	器可能已经失陷。 3写的攻击程序,黑客可	可能借此入侵您的系统。	
😯 修复建议				
建议方案	<ol> <li>隔离或者删除相关的木马文件;</li> <li>2.对系统进行风险排查,并进行安全加固,详情可 【Linux】 https://cloud.tencent.com/document/p 【Windows】 https://cloud.tencent.com/document</li> </ol>	参考如下链接: roduct/296/9604 nt/product/296/9605		

- 可单击隔离,对该文件进行隔离并结束相关进程的操作,该告警处理状态将变为"已隔离"。
- 可登录该主机,找到对应文件,手动进行删除或隔离并结束相关进程,然后在控制台对该告警标记已处理, 该告警处理状态将变为"已处理"。

6. 在文件查杀页面,单击右上角的**查杀设置**,建议开启自动隔离开关,检出恶意文件则立即自动隔离。



查杀设置		×
+		
专业版/旗制	觊厥王机均文狩疋时检测和头时监控,目如隔离切能属于旗舰破切能,建议您 <b>升级破本                                    </b>	
定时扫描	实时监控 NEW 自动隔离	
规则内容		
自动隔离	开启或关闭自动隔离,均需要进行配置,实际生效存在几分钟延迟,请知悉。	
	主机安全将自动隔离检测出的恶意文件,部分恶意文件仍需用户手动确认隔离,建议您检查文件查杀中的告警列表,确保已全部处理。若出现误隔离,请在已隔 离列表中对文件进行恢复。	
	杀掉进程: ✓ 杀掉该文件相关进程,建议勾选	
防护模式	标准模式 重保模式	
	仅针对高置信度的风险进行自动防护,更适合日常安全运营使用。 推荐	
① 说明 ● : - - : - :	<b>]:</b> 并非所有检出的恶意文件均能被自动隔离,部分恶意文件仍需用户手动确认隔离,建议检查文件查察 中的告警列表,确保已全部处理。 若出现误隔离,请在已隔离列表中对文件进行恢复。 开启或关闭自动隔离,均需要进行配置,实际生效存在几分钟延迟。	λĶ

# 热点问题

# 恶意文件在哪里配置告警?

在 告警设置页面, 配置**文件查杀-恶意文件**的告警时间、告警范围和告警项。



主机安全	告警设置					
② 漏洞管理	站内信/短信/邮件等 机器人通知					
◎ 基线管理	() 重要声明					
	产生待处理告警时,主机安全系统 <ul> <li>请确认消息订阅中"主机安全"消</li> </ul>	代会根据配置的告警规则向指 (息设置了接收模式、接收渠)	定的用户发送告誓通知。告誓设置包括如下步骤: 道和接收人(特别说明:主机安全暂不支持语音告警,即使接收渠道中勾选了"语	音"也不会发送语音告警)前往设置 🖸		
◎ 入侵检測 ^	• 配置主机安全各类事件是否告望	8、告警时间及告警项。				
・文件查杀	<ul> <li>告警时间:默认全天24小时,</li> <li>告警项:具体告警内容或告警</li> </ul>	可自定义(告警周期开始时, (事件威胁等级(支持勾选)。	前3条安全事件实时告警,后续每2小时汇总告警1次)			
・ 异常登录						
· 密码破解	入侵检测					
<ul> <li>・ 恶意请求</li> </ul>	告警类型	告誓状态	告鑒时间 ③	告譬主机范围	告警项	
<ul> <li>高危命令</li> <li>本地提权</li> </ul>	文件查杀-恶意文件		●全天 ○ 09:00 ◎ ~ 18:00 ③	全部主机 编辑	✓ 严重 ✓ 高危 中危 低危 提示	
・ 反弹Shell	文件查杀·异常进程		●全天 ○ 09:00 ◎ ~ 18:00 ③	全部主机 编辑	检测到内存中存在正在运行的异常进程	
♥ 高级防御 安全运营	异常登录		●全天 ○ 09:00 ● ~ 18:00 ④	全部主机 编辑	✓ 高危 ✓ 可疑	
	密码破解			全部主机 编辑	登录密码被破解成功	
公置中心	恶意请求		●全天 ○ 09:00 ③ ~ 18:00 ④	全部主机 编辑	服务器请求了恶意域名	0
资 授权管理	高危命令		<ul><li>● 全天</li><li>○ 03:00</li><li>○ 18:00</li><li>○</li></ul>	全部主机 编辑	✔ 高危 🗌 中危 🗌 低危	C
其他应用	本地提权		○全天         03:00         ○         18:00         ○	全部主机 编辑	系统中出现低权限试图提高权限	
	反弹Shell		●全天         09:00         ●         18:00         ●	全部主机 编辑	服务器上出现Shell反向连接	E
三 给产品打个分 の	网页防篡改		●全天 00:00 ~ 18:00 ◎	全部主机 編輯	✔ 篡改成功  ✔ 恢复失败	

## 恶意文件如何设置定期检测?

在 文件查杀页面,单击右上角的查杀设置,打开查杀设置弹窗,进行定时扫描设置。



#### 查杀设置

专业版/旗舰版主机均支持定时检测和实时监控,自动隔离功能属于旗舰版功能,建议您 升级版本 🛽 启用更多安全防护功能。

定时扫描	实时监控 NEW 自动隔离
开启定时扫描	定期扫描主机木马病毒文件,增强安全性
检测模式 🛈	全盘检测 ▼ 除快速检测范围外, 会检测系统所有分区
异常进程检测	深度检测内存中的异常进程,可能造成一定程度的资源占用率升高,请谨慎选择。
检测周期	每隔3天 🔻 02:00 ~ 06:00 🕚
检测范围	
检测范围	● 全部专业版和旗舰版服务器     自选服务器

# 若文件已被删除,再次对进行恶意文件扫描,原告警处理状态会变成什么?

原告警处理状态将变为"已清理"。