漏洞管理服务

产品介绍

文档版本 01

发布日期 2023-12-07

华为云计算技术有限公司

商标声明

HUAWEI和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 初识漏洞管理服务

2 什么是漏洞管理服务

漏洞管理服务（CodeArts Inspector）是针对网站、主机、移动应用、软件包/固件进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理、自定义扫描多项服务。扫描成功后，提供扫描报告详情，用于查看漏洞明细、修复建议等信息。

工作原理

漏洞管理服务具有如下能力：

- Web网站扫描

  采用网页爬虫的方式全面深入的爬取网站url，基于多种不同能力的漏洞扫描插件，模拟用户真实浏览场景，逐个深度分析网站细节，帮助用户发现网站潜在的安全隐患。同时内置了丰富的无害化扫描规则，以及扫描速率动态调整能力，可有效避免用户网站业务受到影响。

- 主机扫描

  经过用户授权（支持账密授权）访问用户主机，漏洞管理服务能够自动发现并检测主机操作系统、中间件等版本漏洞信息和基线配置，实时同步官网更新的漏洞库匹配漏洞特征，帮助用户及时发现主机安全隐患。

- 移动应用安全

  对用户提供的安卓、鸿蒙应用进行安全漏洞、隐私合规检测，基于静态分析技术，结合数据流静态污点跟踪，检测权限、组件、网络等APP基础安全漏洞，并提供详细的漏洞信息及修复建议。

- 二进制成分分析

  对用户提供的二进制软件包/固件进行全面分析，通过解压获取包中所有待分析文件，基于组件特征识别技术、静态检测技术以及各种风险检测规则，获得相关被测对象的组件BOM清单和潜在风险清单，并输出一份专业的分析报告。

3 功能特性

漏洞管理服务可以帮助您快速检测出您的网站、主机、移动应用存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。

- 网站漏洞扫描
  - 具有OWASP TOP10和WASC的漏洞检测能力，支持扫描22种类型以上的漏洞。
  - 支持使用Ajax、JavaScript、Flash等技术构建网站，支持使用Tomcat、Apache、Nginx、IIS等Web容器部署的网站。
  - 扫描规则云端自动更新，全网生效，及时涵盖最新爆发的漏洞。
  - 支持静态页面和动态页面扫描。
  - 支持HTTPS扫描。
- 一站式漏洞管理
  - 提供漏洞修复建议。如果您需要查看修复建议，请购买专业版、高级版或者企业版。
  - 支持下载扫描报告，用户可以离线查看漏洞信息。如果您需要下载扫描报告，请购买专业版、高级版或者企业版。
  - 支持重新扫描。
- 支持弱密码扫描
  - 多场景可用

    支持操作系统(RDP协议、SSH协议)、数据库（如Mysql、Redis）等常见中间件弱口令检测。
  - 丰富的弱密码库

    丰富的弱密码匹配库，模拟黑客对各场景进行弱口令探测。
- 支持端口扫描

  扫描服务器端口的开放状态，检测出容易被黑客发现的“入侵通道”。
- 自定义扫描
  - 支持任务定时扫描。
  - 支持基于用户名密码登录、基于自定义Cookie登录。
  - 支持Web 2.0高级爬虫扫描。
  - 支持自定义Header扫描。

  - 支持手动导入探索文件来进行被动扫描。
- 主机漏洞扫描
  - 支持深入扫描

    通过配置验证信息，可连接到服务器进行OS检测，进行多维度的补丁、已知漏洞、配置检测。

    支持操作系统典型服务协议SSH、SSL/TLS的识别和已知漏洞扫描。
  - 支持内网扫描

    可以通过跳板机方式访问业务所在的服务器，适配不同企业网络管理场景。
  - 支持中间件扫描
    - 丰富的扫描场景

      支持主流Web容器、前台开发框架、后台微服务技术栈的版本漏洞和配置合规扫描。
    - 多扫描方式可选

      支持通过标准包或者自定义安装等多种方式识别服务器的中间件及其版本，全方位发现服务器的漏洞风险。
- 二进制成分分析
  - 全方位风险检测

    对软件包/固件进行全面分析，基于各类检测规则，获得相关被测对象的开源软件、信息泄露、安全配置、安全编译选项等存在的潜在风险。
  - 支持各类应用

    支持对桌面应用（Windows和Linux）、移动应用程序（APK、IPA、Hap等）、嵌入式系统固件等的检测。
  - 专业分析指导

    提供全面、直观的风险汇总信息，并针对不同的扫描告警提供专业的解决方案和修复建议。
- 移动应用安全

  移动应用安全服务能快速扫描您的应用，并提供详细的检测报告，协助您快速定位修复问题。
  - 全自动化测试

    您只需上传Android、HarmonyOS应用文件提交扫描任务，即可输出详尽专业的测试报告。

    支持工信部等4部委的合规要求进行检测，主要检测内容包括隐私声明和行为一致性检测、权限检测、隐私检测、安全问题检测等内容的自动化检测。
  - 详细的测试报告

    详尽的在线测试报告，一键即可下载，报告提供包括问题代码行、修复建议、调用栈信息、违规问题场景截图、关联隐私策略片段等信息。
  - 支持第三方SDK隐私声明解析

    针对第三方SDK隐私声明存在“表格”与“外链”两种展示方式。通过插桩方式获取应用隐私声明的url，继而提取并深度分析隐私声明内容。
  - 支撑鸿蒙应用扫描

    率先支持鸿蒙应用安全漏洞、隐私合规问题扫描。

4 产品优势

扫描全面

涵盖多种类型资产扫描，支持云内外网站、主机漏洞、二进制成分分析和移动应用安全，智能关联各资产，自动发现资产指纹信息，避免扫描盲区。

简单易用

配置简单，一键全网扫描。可自定义扫描事件，分类管理资产安全，让运维工作更简单，风险状况更清晰了然。

高效准确

- 采用Web2.0智能爬虫技术，内部验证机制不断自测和优化，提高检测准确率。
- 时刻关注业界紧急CVE爆发漏洞情况，自动扫描，快速了解资产安全风险。
- 快速排查用户软件包/固件中的开源软件、安全配置等风险。

报告全面

清晰简洁的扫描报告，多角度分析资产安全风险，多元化数据呈现，将安全数据智能分析和整合，使安全现状清晰明了。

5 产品规格差异

漏洞管理服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。

各服务版本支持的计费方式、功能和规格说明如下所示，您可以根据业务需求选择相应的服务版本。

表 5-1 各服务版本计费方式

服务版本	支持的计费方式	说明	价格详情
基础版	● 配额内的服务免费 ● 按需计费	● 基础版配额内仅支持Web网站漏洞扫描（域名个数：5个，扫描次数：5个域名每日总共可以扫描5次）是免费的。 ● 基础版提供的以下功能按需计费： 1. 可以将Web漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持20台主机。	产品价格详情
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。	
高级版	包年/包月		
企业版	包年/包月		

表 5-2 各服务版本功能说明

功能	基础版	专业版	高级版	企业版
常见Web漏洞检测	√	√	√	√

功能	基础版	专业版	高级版	企业版
端口扫描	√	√	√	√
自定义登录方式	√	√	√	√
Web 2.0高级爬虫	√	√	√	√
网站指纹识别	√	√	√	√
扫描任务管理	√	√	√	√
漏洞查看及管理	√	√	√	√
CVE漏洞扫描	×	√	√	√
弱密码检测	×	√	√	√
网页内容合规检测（文字）	×	√	√	√
操作系统漏洞扫描	×	√	√	√
操作系统基线检查	×	√	√	√
中间件基线检查	×	√	√	√
云原生基线扫描	×	√	√	√
查看漏洞修复建议	×	√	√	√
下载扫描报告	×	√	√	√
安全监测（定时扫描）	×	√	√	√
网页内容合规检测（图片）	×	×	×	√
网站挂马检测	×	×	×	√
链接健康检测（死链、暗链、恶意外链）	×	×	×	√
操作系统等保合规检查	×	×	×	√
支持手动探索文件导入	×	×	×	√

表 5-3 各服务版本支持的扫描配额说明

版本	域名/IP个数	扫描次数	单个任务时长	任务优先级	单用户并发扫描数
基础版	Web漏扫：包含5个二级域名或IP:端口。	Web漏扫：5个域名每日总共可以扫描5次	2小时	低	默认Web漏扫最大并发为1个域名。

版本	域名/IP个数	扫描次数	单个任务时长	任务优先级	单用户并发扫描数
专业版	Web漏扫：包含1个二级域名或IP:端口。 主机漏扫：包含20个IP地址。		无限制	高	默认Web漏扫最大并发为3个域名。 默认主机漏扫最大并发为5个IP。
高级版	Web漏扫：默认包含1个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制IP地址个数。		无限制	高	默认Web漏扫最大并发为5个域名。 默认主机漏扫最大并发为10个IP。
企业版	Web漏扫：默认包含5个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制IP地址个数。 **说明** 当默认的扫描配额不能满足您的需求时，您可以通过购买扫描配额包增加扫描配额（一个扫描配额包中包含一个一级域名扫描配额）。		无限制	高	默认Web漏扫最大并发为10个域名。 默认主机漏扫最大并发为20个IP。 **说明** 更高并发需要，请提交工单联系专业工程师为您服务。

说明

一级域名指用户通过华为云或者第三方域名注册商，购买注册的域名。

二级域名指无需购买注册，可直接在一级域名下添加的子域名。

例如：一级域名：example.com, example.com.cn，二级域名：test.example.com, test.example.com.cn，详细请参考域名注册。

6 应用场景

漏洞管理服务主要用于以下场景。

- Web漏洞扫描应用场景

  网站的漏洞与弱点易于被黑客利用，形成攻击，带来不良影响，造成经济损失。

  - 常规漏洞扫描

    丰富的漏洞规则库，可针对各种类型的网站进行全面深入的漏洞扫描，提供专业全面的扫描报告。

  - 最新紧急漏洞扫描

    针对最新紧急爆发的CVE漏洞，安全专家第一时间分析漏洞、更新规则，提供快速专业的CVE漏洞扫描。

- 主机漏洞扫描应用场景

  运行重要业务的主机可能存在漏洞、配置不合规等安全风险。

  - 支持深入扫描

    通过配置验证信息，可连接到服务器进行OS检测，进行多维度的漏洞、配置检测。

  - 支持内网扫描

    可以通过跳板机方式访问业务所在的服务器，适配不同企业网络管理场景。

- 弱密码扫描应用场景

  主机或中间件等资产一般使用密码进行远程登录，攻击者通常使用扫描技术来探测其用户名和弱口令。

  - 多场景可用

    支持操作系统(RDP协议、SSH协议)、数据库（如Mysql、Redis）等常见中间件服务的弱口令检测。

  - 丰富的弱密码库

    丰富的弱密码匹配库，模拟黑客对各场景进行弱口令探测。

- 中间件扫描应用场景

  中间件可帮助用户灵活、高效地开发和集成复杂的应用软件，一旦被黑客发现漏洞并利用，将影响上下层安全。

  - 丰富的扫描场景

    支持主流Web容器、前台开发框架、后台微服务技术栈的版本漏洞和配置合规扫描。

  - 多扫描方式可选

    支持通过标准包或者自定义安装等多种方式识别服务器的中间件及其版本，全方位发现服务器的漏洞风险。

- 内容合规检测应用场景

  当网站被发现有不合规言论时，会给企业造成品牌和经济上的多重损失。

  - 精确识别

    同步更新时政热点和舆情事件的样本数据，准确定位各种涉黄、涉暴涉恐、涉政等敏感内容。

  - 智能高效

    对文本、图片内容进行上下文语义分析，智能识别复杂变种文本。

- 二进制成分分析应用场景

  产品包或固件中因不当使用开源软件、配置不合规等会产生漏洞或合规性风险，及时的发现和修复相关问题可以减少被攻击者利用的风险。

  - 全方位风险检测

    对产品包/固件进行全面分析，基于各类检测规则，获得相关被测对象的开源软件、信息泄露、安全配置、安全编译选项等存在的潜在风险。

  - 支持各类应用

    支持对桌面应用（Windows和Linux）、移动应用程序（APK、IPA、Hap等）、嵌入式系统固件等的检测。

  - 专业分析指导

    提供全面、直观的风险汇总信息，并针对不同的扫描告警提供专业的解决方案和修复建议。

- 移动应用安全

  - 企业自检或通报后自查

    适用于各类APP发版自检，及通报整改后自查，服务提供详细精确的报告协助企业快速定位修复问题，达到监管合规要求。

  - 审核机构APP合规审查

    紧贴各类监管规范，提供高效的自动化检测服务，能快速识别存在违规行为的APP。

7 使用约束

网站扫描域名/IP

漏洞管理服务是通过公网访问域名/IP地址进行扫描的，请确保该目标域名/IP地址能通过公网正常访问。

扫描 IP 加入网站扫描白名单

如果您的网站设置了防火墙或其他安全策略，将导致漏洞管理服务的扫描IP被当成恶意攻击者而误拦截。因此，在使用漏洞管理服务前，请您将以下扫描IP添加至网站访问的白名单中：

119.3.232.114，119.3.237.223，124.70.102.147，121.36.13.144，124.70.109.117，139.9.114.20，119.3.176.1

8 计费说明

本小节主要介绍漏洞管理服务的计费说明，包括计费项、计费模式、续费等。详细信息请参考产品价格详情。

计费项

漏洞管理服务根据您的服务版本，扫描配额包的个数和购买时长计费。

表 8-1 计费项信息

计费项目	计费说明
服务版本（必选）	按购买的服务版本（基础版、专业版、高级版或企业版）计费。
扫描配额包	按购买的个数计费。
购买时长	提供包年/包月和按需计费的购买模式。

计费模式

漏洞管理服务提供按需计费和包年/包月两种计费模式，用户可以根据实际需求选择计费模式。

表 8-2 各服务版本计费方式

服务版本	支持的计费方式	说明	价格详情
基础版	• 配额内的服务免费 • 按需计费	• 基础版配额内仅支持Web网站漏洞扫描（域名个数：5个，扫描次数：每日5次）是免费的。 • 基础版提供的以下功能按需计费： 1. 可以将Web漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持20台主机。	产品价格详情
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。不限制扫描次数。	
高级版			
企业版			

变更配置

- 域名配额扩容：当您的业务需求增加，可在计费周期内“扩容”域名的扫描配额包。支持扩容**专业版配额**、**高级版配额**以及**企业版配额**。不支持多个版本同时存在。
- 专业版升级为高级版：当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额全部升级为一级域名配额，可以直接将**专业版**升级为**高级版**。
- 退订：购买漏洞管理服务的扫描配额包后，如需停止使用，请到费用中心执行退订操作。

续费

扫描配额包到期后，您可以进行续费以延长扫描配额包的有效期，也可以设置到期自动续费。请参见续费管理。

到期与欠费

包周期资源开通成功后，如果没有按时续费，公有云平台会提供一定的保留期，详细信息请参见“保留期”。

欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，账号将进入欠费状态，需要在约定时间内支付欠款，详细操作请参考欠费还款。

FAQ

更多计费相关FAQ，请参见漏洞管理服务常见问题。

9 个人数据保护机制

为了确保网站访问者的个人数据（例如用户名、密码等）不被未经过认证、授权的实体或者个人获取，漏洞管理服务通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

漏洞管理服务收集及产生的个人数据如表9-1所示。

表 9-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
域名/IP地址	在添加域名时，由用户在界面输入。	是	是
用户名（网站登录）	在设置账号密码登录方式时，由用户在界面输入。	是	否
密码（网站登录）	在设置账号密码登录方式时，由用户在界面输入。	是	否
cookie值	在设置cookie登录方式时，由用户在界面输入。	是	否 cookie值可能不含有用户的个人信息。

存储方式

除域名/IP地址明文保存外，其他字段加密存储。

访问权限控制

用户只能查看自己业务的相关信息。

日志记录

用户个人数据的所有非查询类操作，包括创建、删除域名等，漏洞管理服务都会记录审计日志并上传至云审计服务（CTS），用户仅可以查看自己的审计日志。

10 漏洞管理服务权限管理

如果您需要对华为云上购买的漏洞管理服务资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有漏洞管理服务的使用权限，但是不希望这些员工拥有删除漏洞管理服务等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用漏洞管理服务，但是不允许删除漏洞管理服务的权限，控制员工对漏洞管理服务资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用漏洞管理服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

漏洞管理服务权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

漏洞管理服务部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问漏洞管理服务时，需要先切换至授权区域。

如**表10-1**所示，包括了漏洞管理服务的所有系统角色。由于华为云各服务之间存在业务交互关系，漏洞管理服务的角色依赖其他服务的角色实现功能。因此给用户授予漏洞管理服务的角色时，需要同时授予依赖的角色，漏洞管理服务的权限才能生效。

表 10-1 漏洞管理服务系统角色

角色名称	描述	依赖关系
VSS Administrator	漏洞管理服务的管理员权限。	依赖Tenant Guest和Server Administrator角色。 ● Tenant Guest：全局级角色，在全局项目中勾选。 ● Server Administrator：项目级角色，在同项目中勾选。

相关链接

- **IAM产品介绍**
- **创建用户组、用户并授予CodeArts Inspector权限**

11 与其他服务的关系

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为漏洞管理服务提供了权限管理的功能。需要拥有VSS Administrator权限的用户才能使用漏洞管理服务。

如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参见《统一身份认证服务用户指南》。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录了漏洞管理服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。云审计服务支持的漏洞管理服务操作列表如表11-1所示。

表 11-1 云审计服务支持的漏洞管理服务操作列表

操作名称	资源类型	事件名称
网站		
创建域名	domain	createDomain
删除域名	domain	deleteDomain
编辑域名	domain	editDomain
免认证/一键认证	domain	authenticateDomain
快捷认证	domain	authorizeDomain
创建漏洞扫描任务	scan	createScanTask
创建内部漏洞扫描任务	scan	createInnerScanTask
重启漏洞扫描任务	scan	restartScanTask
取消漏洞扫描任务	scan	cancelScanTask
编辑漏洞扫描任务	scan	editScanTask

操作名称	资源类型	事件名称
创建订阅套餐	resource	createPurchaseOrder
更新订阅套餐	resource	createAlterOrder
批量更新订阅套餐	resource	createBatchAlterOrder
新用户注册	resource	createVSSResource
删除监测任务	monitor	deleteMonitorJob
暂停监测任务	monitor	pauseMonitorJob
恢复监测任务	monitor	resumeMonitorJob
忽略漏洞	vuln	addVulnFalsePositive
取消忽略漏洞	vuln	deleteVulnFalsePositive
生成网站扫描报告	report	generateWebScanReport
下载网站扫描报告	report	downloadWebScanReport
主机		
添加主机	host	addHost
删除主机	host	deleteHost
编辑主机	host	editHost
更换分组	host	changeHostGroup
新增主机组	host	addHostGroup
编辑主机组	host	editHostGroup
删除主机组	host	deleteHostGroup
创建主机扫描任务	scan	createHostScanTask
取消主机扫描任务	scan	cancelHostScanTask
添加跳板机	jumper	saveJumperServer
编辑跳板机	jumper	editJumperServer
删除跳板机	jumper	deleteJumperServer
添加smb授权	credential	saveSmbCredential
编辑smb授权	credential	editSmbCredential
删除smb授权	credential	deleteSmbCredential
添加ssh授权	credential	saveSshCredential
编辑ssh授权	credential	editSshCredential
删除ssh授权	credential	deleteSshCredential

操作名称	资源类型	事件名称
添加租户委托	tenant	addTenantAgency
删除租户委托	tenant	deleteTenantAgency
清空资源	cleanup	resourcesCleanUp
忽略漏洞	vuln	addVulnFalsePositive
取消忽略漏洞	vuln	deleteVulnFalsePositive
生成主机扫描报告	report	generateHostScanReport
下载主机扫描报告	report	downloadHostScanReport