TencentOS Server

版本与支持

腾讯云

文档目录

版本与支持
版本说明

最近更新时间：2024-09-27 15:44:41

TencentOS Server 2

TencentOS Server 2 或 tlinux2，全面兼容 CentOS 7，当前产品线主要有 TencentOS Server 2.4。

TencentOS Server 3

TencentOS Server 3 或 tlinux3，全面兼容 CentOS 8，当前产品线主要有 TencentOS Server 3。

TencentOS Server 4

内置 Linux 6.6 LTS 稳定版本内核，其内核及用户态软件均基于 upstream 社区独立演进，自主选型和维护，不再依赖任何第三方发行版。当前产品先主要 TencentOS Server 4。

版本支持说明

最近更新时间：2024-09-27 15:44:41

版本支持说明

TencentOSServer 生命周期：10+3年，保障长期稳定支持。

阶段1（Full Support 约5年）	阶段2（Maintenance 约5年）	阶段3（Extended Lifecycle 约3年）

每个大版本的维护周期10年，按需可延长3年（需叠加购买），分三个阶段。阶段说明如下表：

阶段	定义	时长
全支持阶段（阶段1）	包括 Critical 和 Important 的安全漏洞修复，紧急高优的 bug 修复，操作系统软件功能增强与优化、不需要大范围改动代码的新硬件特性支持，云上镜像或 yum源上 ISO 小版本会持续保持更新。腾讯云会提供完全的 OS 技术支持。	5年
维护支持阶段（阶段2）	包括 Critical 和 Important 的安全漏洞修复，紧急高优的 bug 修复，一般情况下不再增加新的操作系统软件功能、不再支持新的硬件特性，云上镜像或 yum 源上 ISO 小版本会持续保持更新。	5年
延长服务阶段（阶段3）	仅包括 Critical 和 Important 的安全漏洞修复以及紧急高优的 bug 修复，不再提供新的操作系统软件功能、不再支持新的硬件特性，云上镜像或 yum 源 ISO 小版本不再更新。	3年

TencentOS Server 2.4

GA 版本发布	阶段1结束（EOFS）	阶段2（EOM）	阶段3（EOS）
2019.12.31	2024.12.31	2029.12.31	2032.12.31

TencentOS Server 3

GA 版本发布	阶段1结束（EOFS）	阶段2（EOM）	阶段3（EOS）
2019.12.31	2024.12.31	2029.12.31	2032.12.31

TencentOS Server 4

GA 版本发布	阶段1结束（EOFS）	阶段2（EOM）	阶段3（EOS）

2023.4.30	2028.4.30	2033.4.30	2036.4.30

- 每4年左右一个大版本，腾讯为每个大版本提供阶段1、2的常规服务（10年），按需提供阶段3的延长生命服务（ELS）。
- 每个大版本期间，每3-4年发布一个小版本，按需为小版本提供生命延长更新服务（LLUS）。

漏洞服务规则

最近更新时间：2024-09-19 15:24:51

TencentOS 漏洞服务规则

本规则适用于 TencentOS 所有产品，旨在帮助 TencentOS 用户和社区成员理解 TencentOS 如何评估、响应和披露系统中的安全漏洞。

漏洞定义

漏洞（Vulnerability）指的是系统中存在的弱点或缺陷，漏洞可被利用对系统或其应用数据的机密性、完整性、可用性造成威胁。

漏洞上报

TencentOS 安全运营团队通过多种渠道实时监控世界范围内开源社区的安全态势。与此同时，我们也欢迎用户主动向我们报告发行版中存在的安全漏洞。
如果您在 TencentOS 产品中发现了疑似的安全漏洞，我们希望您将漏洞报告给我们，并配合我们以负责任的方式修复和披露该问题。
但对于以下几种情形，建议您在报告前首先联系维护团队进行咨询：

- 您仅仅希望得到与安全有关的技术帮助。
- 您所要报告的缺陷与安全无关（无法被利用以破坏系统的安全性）。

漏洞上报方式

根据《中华人民共和国网络安全法》，我们不建议任何人直接公开有关 TencentOS 安全漏洞的细节，如需报告安全漏洞，请发送邮件至 TencentOS 安全应急响应邮箱（tencentos_secure@tencent.com），我们会在第一时间响应。
由于漏洞信息较为敏感，建议您在发送邮件时，使用 PGP 方式加密（加密方法和密钥详见附录，非强制）。

漏洞上报内容

为了形成有效的沟通，我们推荐您按照以下格式撰写漏洞上报邮件（对于不确定的内容，可填写不确定）：

- 漏洞标题：一句话概括漏洞内容，直接体现漏洞类型和影响的组件，例如 **sudo 的 sudoedit 命令存在堆溢出提权漏洞。**
- 自我介绍：请简单介绍您自己或您所在的组织，以便我们与您取得联系。
- 漏洞基本信息。
- 漏洞类型：为漏洞选择一个分类，建议参考 CWE 漏洞分类标准（CWE List Version 4.15）。
- 漏洞等级：请提供基于 CVSS v3.1 标准的漏洞自我评级结果和理由。
- 受影响的系统和组件：请提供受影响的 TencentOS 系统版本（可通过 `cat /etc/tencentos-release` 命令确定，例如 TencentOS Server 3.2），以及受影响的软件包（例如 sudo-1.8.29-

7.tl3.x86_64）。

- 最早发现时间：请提供已知的最早发现该漏洞的时间。
- 原始信息来源：请描述漏洞信息来源，是自己发现，还是从其他来源获取的。
- 是否已经向其他组织报告：如果是，请提供该组织的名称，以及报告时间。
- 漏洞详细说明。
- 漏洞概述：请用几句话简要描述该漏洞。
- 漏洞影响：请描述该漏洞的影响范围和可能造成的危害。
- 漏洞复现过程：请采用图文形式，尽可能详细地描述漏洞发现过程，确保读者可按照步骤完成漏洞的复现。
- 攻击代码（POC）：可在附件中提供，或提供相应的链接。
- 修复建议：欢迎提供漏洞的修复建议，可通过文字说明、修复补丁、伪代码等形式。

漏洞上报响应

TencentOS 安全运营团队承诺为漏洞上报提供最及时的响应：

- 我们会在1个工作日内确认收到安全漏洞报告，在3个工作日内完成初步评估并回复上报的安全问题，后续会随时向上报者同步漏洞处理的进展。
- 对于尚未对外公开的漏洞，我们将在收到信息的2天内向工信部网络安全威胁和漏洞信息共享平台报告并通知软件上游社区，除此以外，我们不会在未经报告者许可的情况下，向任何第三方提供漏洞信息。
- 我们不隶属于任何第三方漏洞赏金计划，也暂时不向我们产品中的漏洞报告提供赏金，但我们会在征得报告者同意的前提下，在安全公告中致谢。

漏洞评估

漏洞带来的影响与受影响组件的版本、使用方式、平台以及编译方式等相关，因此 TencentOS 安全团队要基于具体环境对漏洞做重评估，评估内容包括但不限于：

- 我们是否在发布版本中携带了受影响的软件包。
- 如果携带了受影响的软件包，哪些发布版本受影响。
- 漏洞的严重程度和影响是怎样的。
- 是否有现存的 CVE ID 与之对应。

我们采用国际通用的漏洞评分标准 CVSS V3.1 对漏洞进行严重性评估（关于该标准的详细说明，详情请参见 Common Vulnerability Scoring System）。CVSS V 3.1 通过以下指标组合评估一个漏洞的影响：

- 可利用指标。
- 攻击向量（AV）：衡量受攻击系统的**远程性**以及利用漏洞的方式。
- 攻击复杂度（AC）：衡量执行攻击的难度以及攻击成功所需的因素。
- 用户交互（UI）：判断攻击是否需要用户参与。
- 权限需要（PR）：记录进行攻击所需的用户身份验证级别。
- 范围（S）：判断攻击者是否可以影响超出其安全域/权限范围的组件。
- 受影响指标。

- 机密性（C）：衡量未授权用户是否可以访问信息资源以及可访问的程度。
- 完整性（I）：衡量漏洞对数据可信度和真实性的影响。
- 可用性（A）：衡量漏洞对合法授权用户访问数据或服务的影响。

根据 CVSS v3.1 打分，我们将漏洞按严重程度划分为以下五个等级：

严重等级	CVSS 评分
致命（Critical）	9.0–10.0
高（High）	7.0–8.9
中（Medium）	4.0–6.9
低（Low）	0.1–3.9
无（None）	0.0

我们将根据漏洞严重程度等级决定是否修复漏洞以及为此投入的资源。

漏洞披露

在安全漏洞修复后，TencentOS 将以安全公告的形式对外公开，公告内容包括但不限于：

- 漏洞链接：TencentOS Server Security Advisories 。
- 受影响组件版本和修复版本。
- 修复或规避措施。
- 漏洞对应的缺陷管理系统链接。

一旦有修复或规避措施，我们就会尽快将漏洞对外披露出来，具体披露时间由 TencentOS 安全团队和漏洞提交者协商决定。

为帮助管理员快速决定是否进行更新，以及何时更新，我们将安全公告分为四个等级：

优先级	解释
严重（Critical）	该评级针对可被远程未经身份验证的攻击者无需用户交互就轻松利用并导致系统破坏（任意代码执行）的漏洞。这些是蠕虫可利用的漏洞类型。需要经过身份验证的远程用户、本地用户或依赖罕见配置的漏洞不属于严重级别。
重要（Important）	该评级针对容易危及资源的机密性、完整性或可用性的漏洞。这些漏洞允许本地用户获得特权，允许未经身份验证的远程用户查看本应通过身份验证保护的资源，允许经过身份验证的远程用户执行任意代码，或允许未经身份验证的远程用户在没有用户交互的情况下造成拒绝服务。
中等（Moderate）	该评级针对可能更难利用但在某些情况下仍可能导致资源机密性、完整性或可用性受损的缺陷。这些漏洞可能会产生严重影响或重要影响，但根据对缺陷的技术评估，它们不太容易被利用，或者只在很罕见的配置下有影响。无论是否要求用户交互，可造成基本系统服

	务（例如内核、systemd、polkit、dbus，...）在本地间断（服务需要重新启动）拒绝服务的漏洞也应该被评为“中等”。
低（Low）	此评级适用于所有其他具有安全影响的问题。这些漏洞类型被认为不太可能被利用，或者成功利用产生的影响很小。

为保护用户的安全，在进行调查、修复和发布安全公告之前，TencentOS 都不会公开披露和讨论产品中存在的安全问题。

TencentOS 对漏洞的披露方式和日期享有最终解释权。