# TencentOS Server

# 产品动态

腾讯云

# 文档目录

# 产品动态
# 公告
# Sudo 提权漏洞公告（CVE-2025-32462、CVE-2025-32463）

最近更新时间：2025-07-03 17:56:52

近期，TencentOS 安全团队监测到 CVE 官网披露漏洞（CVE-2025-32462、CVE-2025-32463），漏洞受影响组件为 sudo，影响 TencentOS Server 2、TencentOS Server 3、TencentOS Server 4的产品。监测到漏洞情报后，安全团队第一时间对漏洞进行分析和修复。

> **注意：**
> 若您已使用 TencentOS，建议您及时开展风险自查，如受影响，请及时根据 TencentOS 为用户提供的漏洞修复解决方案进行防护，确保您的系统安全。

## 1. 漏洞详情

### CVE-2025-32462

该漏洞源于 Linux 系统 sudo 组件的配置逻辑缺陷。攻击者可通过构造含通配符或未验证的主机名，在非预期主机上执行命令，绕过 sudoers 文件的主机限制，结合命令执行实现本地提权。

利用条件：
本地攻击者（包括通过 SSH 获得本地 Shell 权限的用户）在系统使用共享 sudoers 配置（LDAP/SSSD）或多主机分发规则时，通过 `sudo -h<主机名>` 命令绕过当前主机的策略限制，执行未授权的特权操作（例如修改配置或挂载设备），导致服务瘫痪或数据窃取。

### CVE-2025-32463

该漏洞源于 sudo 因不当实现--chroot（-R）选项引发的高危本地提权漏洞。攻击者可利用该选项指定自定义 chroot 目录，通过操控目录内的 `/etc/nsswitch.conf` 文件，强制 sudo 加载攻击者控制的共享库，从而以 root 权限执行任意命令。

利用条件：
攻击者通过本地账号在可控目录创建恶意 `/etc/nsswitch.conf` 文件，利用 sudo -R<目录>触发 chroot 环境加载该配置，使 sudo 以 root 权限加载伪造的 NSS 共享库（例如 libnss *.so），直接获取完整系统控制权。

## 2. 受影响自查指南

## 自查 CVE-2025-32462：

登录环境并执行以下命令进行检查：

**确认 sudo 组件版本**

```
rpm -q sudo  # 确认sudo组件版本
```

**受影响组件版本：**

- TencentOS Server 4：sudo < 1.9.15p5-5.tl4
- TencentOS Server 3：sudo < 1.9.5p2-1.tl3.1
- TencentOS Server 2：sudo < 1.8.23-10.tl2.3.1

## 自查 CVE-2025-32463：

1. **确认系统版本**

   ```
   cat /etc/os-release | grep -w VERSION
   ```

   若 OS 版本为 TencentOS Server 4，则继续排查，**TencentOS Server 2/3 不受影响**。
2. **确认 sudo 组件版本**

   ```
   rpm -q sudo  # 继续确认sudo组件版本
   ```

   **受影响组件版本：**TencentOS Server 4：sudo < 1.9.15p5-5.tl4

# 3. 临时缓解措施

## CVE-2025-32462 的缓解措施

该漏洞没有缓释措施，需要升级 sudo 版本解决。

## CVE-2025-32463 的缓解措施

该漏洞没有缓释措施，需要升级 sudo 版本解决。

# 4. 漏洞修复方案

若您的版本在受影响范围内，TencentOS Server 已在第一时间将官方漏洞补丁推送至系统仓库，您可通过升级命令，将组件升级至安全版本，以修复漏洞。

## 修复指引

- **CVE-2025-32462 修复方式**

| 系统版本 | 修复方式 |
| --- | --- |
| TencentOS Server 2 | 升级修复，执行命令：<br>`yum update sudo;` |
| TencentOS Server 3.1 | 推荐方案一：先升级至 TencentOS Server 3.3，再更新 sudo 版本。<br>为持续提升产品体验、功能优化，推荐您先升级至 TencentOS Server 3.3版本，再进行漏洞修复，彻底升级详情请参见 升级说明 。<br>您也可以参照下述步骤进行：<br>步骤一：<br>• x86环境：依次执行以下命令<br>`wget https://mirrors.tencent.com/tlinux/3.3/BaseOS/x86_64/os/Packages/tencentos-release-3.3-7.tl3.x86_64.rpm`<br>`rpm -Uvh tencentos-release-3.3-7.tl3.x86_64.rpm`<br>• ARM 环境：依次执行以下命令<br>`wget https://mirrors.tencent.com/tlinux/3.3/BaseOS/aarch64/os/Packages/tencentos-release-3.3-7.tl3.aarch64.rpm`<br>`rpm -Uvh tencentos-release-3.3-7.tl3.aarch64.rpm`<br>步骤二：升级 sudo 版本，执行命令：<br>`yum update sudo;` |

| | |
|---|---|
| | 方案二：直接更新 sudo 版本。<br>若暂时不考虑升级至 TencentOS Server 3.3，可执行以下命令修复：<br>`yum update sudo;` |
| TencentOS Server 3.3 | 升级修复，执行命令：<br>`yum update sudo;` |
| TencentOS Server 4 | 升级修复，执行命令：<br>`dnf update sudo;` |

- **CVE-2025-32463 修复方式**

| 系统版本 | 修复方式 |
|---|---|
| TencentOS Server 4 | 升级修复，执行命令：<br>`dnf update sudo;` |

## 修复确认

执行以下命令，查看 sudo 版本，确认是否成功修复。

```
rpm -qa | grep -E "^sudo-[0-9]"
```

已修复版本信息如下：

- TencentOS Server 2：sudo-1.8.23-10.tl2.3.1
- TencentOS Server 3：sudo-1.9.5p2-1.tl3.1
- TencentOS Server 4：sudo-1.9.15p5-5.tl4

更多安全内容请参见 安全公告 。

# 关于 Linux 本地提权漏洞的风险提示

最近更新时间：2025-06-23 14:50:42

近期，TencentOS 安全团队监测到 CVE 官网披露漏洞（CVE-2025-6018、CVE-2025-6019 ），漏洞受影响组件分别为（PAM、libblockdev、udisks ），其中 PAM（Pluggable Authentication Modules ）不受影响，libblockdev、udisks 影响 TencentOS Server 2、TencentOS Server 3、TencentOS Server 4的产品。监测到漏洞情报后，安全团队第一时间对漏洞进行分析和修复。

> **注意：**
> 若您已使用 TencentOS，建议您及时开展风险自查，如受影响，请及时根据 TencentOS 为用户提供的漏洞修复解决方案进行防护，确保您的系统安全。

## 漏洞详情

### CVE-2025-6018

该漏洞源于 Linux 系统 PAM 身份验证模块的配置逻辑缺陷。攻击者可通过普通 SSH 访问绕过 polkit 策略限制，构造特定环境变量组合，在调用 pam_systemd.so 认证模块前利用 pam_env.so 模块开启 user_readenv 选项，从而诱导系统误判网络登录用户具备物理终端权限（allow_active ），最终获得 root 级控制台访问权限。

利用条件：

- 系统启用 PAM 模块并配置允许网络用户通过 SSH 进行身份验证。
- pam_env.so 模块加载顺序早于 pam_systemd.so（常见于默认配置 ）。
- 未对 user_readenv 环境变量进行严格限制。

TencentOS 上 PAM 默认配置下不受影响，为避免用户自定义配置引入漏洞，本文提供了 PAM 组件的受影响排查方法。

### CVE-2025-6019

该漏洞源于 libblockdev 组件在权限检查机制中的逻辑缺陷。攻击者可通过构造恶意块设备操作请求，绕过 udisks 守护进程的权限验证逻辑，利用其 allow_active 参数触发 libblockdev 未正确校验的 API 接口，从而以普通用户身份直接获取 root 权限。

利用条件：

- 系统使用受漏洞影响的 libblockdev 3.1.0及 udisks 2 2.10.0组件。

- udisks 守护进程默认启用 allow_active 参数（常见于默认配置）。
- 依赖 D-Bus 消息总线服务进行进程间通信（默认启用）。

成功利用此漏洞后，攻击者可完全控制目标主机，任意篡改服务器配置（如关闭数据库服务）、窃取核心数据（客户信息/云凭证）、植入持久化后门（业务重启仍可维持控制），并通过内网横向移动进一步扩散影响，最终导致业务中断、合规处罚及供应链信任链崩坏。

# 受影响自查指南

## 自查CVE-2025-6018

若用户自定义修改了 PAM 组件配置，可登录环境并执行以下命令进行检查：

1. 确认是否安装组件 PAM：

```
rpm -qi pam   #检查是否安装 PAM
```

   - 若未安装则不受影响。
   - 若已安装需要执行下一步

2. 已安装 PAM 情况下，检查设置：

```
#若已安装 PAM，请检查有无如下设置：
grep -nir "user_readenv" /etc/pam.d/
```

   - 若输出结果为空或 user_readenv 不为1，则不受影响。
   - 若 user_readenv 为1则受影响，请立即修复或采取临时缓解措施。

## 自查CVE-2025-6019

1. 执行如下命令查询 udisks2 是否安装：

```
rpm -q --qf '%{version}-%{release}\n' udisks2
```

   - 若输出 "package udisks2 is not installed"或无版本信息，则未安装不受影响。
   - TencentOS Server 4环境下，版本号≤ 2.10.0-5.tl4 则受影响，需要执行漏洞修复方案。
   - TencentOS Server 3环境下，版本号≤ 2.9.0-16.tl3 则受影响，需要执行漏洞修复方案。
   - TencentOS Server 2环境下，版本号≤ 2.8.4-1.tl2 则受影响，需要执行漏洞修复方案。

2. 执行如下命令查询 libblockdev 是否安装：

```
rpm -q --qf '%{version}-%{release}\n' libblockdev
```

- 若输出 "package libblockdev is not installed"或无版本信息，则未安装不受影响。
- TencentOS Server 4环境下，版本号≤ 3.1.0-3.tl4 则受影响，需要执行漏洞修复方案。
- TencentOS Server 3环境下，版本号≤ 2.28-6.tl3 则受影响，需要执行漏洞修复方案。
- TencentOS Server 2环境下，版本号≤ 2.18-5.tl2 则受影响，需要执行漏洞修复方案。

受影响组件版本：
TencentOS Server 4： libblockdev <=3.1.0-3 和 udisks2 <= 2.10.0-5
TencentOS Server 3：libblockdev <=2.28-6 和 udisks2 <= 2.9.0-16
TencentOS Server 2：libblockdev <=2.18-4 和 udisks2 <= 2.8.4-1

# 漏洞修复方案

若您的版本在受影响范围，TencentOS Server yum 源已在第一时间将合入了官方漏洞补丁的包推送至系统仓库，您可通过升级相关应用至安全版本，以修复漏洞。修复指引如下：

## CVE-2025-6018修复方式

| 系统版本 | 修复方式 |
| --- | --- |
| TencentOS Server 4<br>TencentOS Server 3<br>TencentOS Server 2 | TencentOS Server 默认不配置 user_readenv，不受影响，如用户自查中发现设置 user_readenv=1，则修改为设置 user_readenv=0，或直接删除，修改后重启 sshd 服务（ `sudo systemctl restart sshd` ）以应用配置变更。<br>**警告：**<br>注意：此步骤可能造成业务中断，请挑选合适时间尽快执行！ |

## CVE-2025-6019修复方式

| 系统版本 | 修复方式 |
| --- | --- |

| | |
|---|---|
| TencentOS Server 4<br>TencentOS Server 3 | 升级并重启服务修复，执行以下命令：<br>`dnf update libblockdev udisks2`<br>重启服务：<br>`systemctl restart udisks2`<br>**警告：**<br>注意：此步骤可能造成业务中断，请挑选合适时间尽快执行！ |
| TencentOS Server 2 | 升级并重启服务修复，执行以下命令：<br>`yum update libblockdev udisks2`<br>重启服务：<br>`systemctl restart udisks2`<br>**警告：**<br>注意：此步骤可能造成业务中断，请挑选合适时间尽快执行！ |

## 修复后验证：

执行如下命令，确认已成功安装了修复后的 libblockdev、udisks2包。

```
rpm -qa | grep -E "^libblockdev-[0-9]|^udisks2-[0-9]"
```

返回具体版本如下，则表明修复成功：

- TencentOS Server 4：libblockdev-3.1.0-4.tl4.x86_64、udisks2-2.10.0-6.tl4.x86_64
- TencentOS Server 3：libblockdev-2.28-6.tl3.1.x86_64、udisks2-2.9.0-16.tl3.1.x86_64
- TencentOS Server 2：libblockdev-2.18-5.tl2.1.x86_64、udisks2-2.8.4-1.tl2.1.x86_64

# 规避措施

## CVE-2025-6019的规避措施

如果您使用的 libblockdev 及 udisks 组件是老版本，或者不方便升级到最新版本时，可使用如以下命令进行缓解：
udisks为系统重要服务，如果 udisks 服务非必要，可临时关闭并屏蔽 udisks 服务。

```
systemctl stop udisks2.service
```

```
systemctl mask udisks2.service
```

判断措施是否执行成功，完成漏洞规避：

```
systemctl status udisks2.service
```

当 Active 状态为 inactive（服务未运行）表示成功屏蔽。

更多安全内容请参考安全公告地址：https://mirrors.tencent.com/tlinux/errata/cve.xml 。

# 关于 Tomcat 远程代码可执行漏洞的风险提示

最近更新时间：2025-03-13 18:24:12

## 背景介绍

近期，TencentOS 安全团队监控到 Apache Tomcat 组件存在远程代码执行漏洞（CVE-2025-24813）。监控到漏洞情报后，安全团队第一时间对漏洞进行分析和修复。
Apache Tomcat 是一个开源的 Java Web 应用服务器，它实现了 Java Servlet 和 JavaServer Pages (JSP) 规范。Tomcat 支持多种功能，包括 HTTP/HTTPS 服务、AJP 连接器、以及对 Servlet 和 JSP 的支持，使其成为开发和部署 Java Web 应用程序的理想选择。
若您已使用 Apache Tomcat 软件，建议您及时开展风险自查，如受影响，请及时根据 TencentOS 为用户提供的漏洞修复解决方案进行防护，确保您的系统安全。

## 漏洞详解

攻击者利用 Apache Tomcat 处理部分 PUT 请求时的逻辑缺陷，构造特殊的 HTTP PUT 请求将路径分隔符替换为“.”，上传恶意序列化文件至默认会话存储目录，且目标系统同时启用 DefaultServlet 写入功能（默认禁用）、开启 partial PUT（默认启用）、使用文件会话持久化默认路径且存在反序列化漏洞库（如 Commons-Collections 3.x），则可触发远程代码执行（RCE），导致服务器被完全控制、敏感数据泄露（如安全配置文件凭据）或业务中断。

## 受影响自查指南

自查系统是否安装 Apache Tomcat，若未安装，则漏洞不涉及。

```
[root@tencentos] sudo rpm -qa | grep tomcat
```

受影响组件版本：

- 11.0.0-M1 <= Apache Tomcat <= 11.0.2
- 10.1.0-M1 <= Apache Tomcat <= 10.1.34
- 9.0.0.M1 <= Apache Tomcat <= 9.0.98

## 修复方案

若您的版本在受影响范围内，TencentOS yum 源已在第一时间将合入了官方漏洞补丁的包推送至系统仓库，您可通过升级相关应用至安全版本，以修复漏洞。
修复指引：
1. 执行如下命令，安装修复后的 tomcat 包。

```
[root@tencentos] sudo yum clean all
[root@tencentos] sudo yum makecache
[root@tencentos] sudo yum update -y tomcat
```

2. 执行如下命令，确认已成功安装了修复后的 tomcat 包。

```
[root@tencentos] sudo rpm -q tomcat
```

具体版本如下：

- TencentOS Server V4：tomcat-9.0.86-8.tl4.1.noarch
- TencentOS Server V3：tomcat-9.0.87-1.tl3.3.noarch

> ⚠ **注意：**
> 此步骤可能造成业务中断，请挑选合适时间尽快执行！

3. 执行如下命令，重启 tomcat 服务。

```
[root@tencentos] sudo systemctl restart tomcat
```

更多安全内容请参见安全公告地址：TencentOS Server Security Advisories 。

## 规避措施

如果您使用的 Apache Tomcat 是老版本，或者不方便升级到最新版本的 Apache Tomcat 时，可使用如下方式进行规避：

1. 排查 `/etc/tomcat/web.xml` 文件，设置 DefaultServlet 的 readonly 为 true，若无此配置则无需处置。
2. 排查 `/etc/tomcat/web.xml` 文件，设置 DefaultServlet 的 allowPartialPut 为 false，若无此配置需要手动添加。
3. tomcat 的文件会话持久化开启状态下，在 `context.xml` 文件中修改默认的会话存储位置。

   打开 `/etc/tomcat/context.xml` 文件，有如下配置代表开启文件会话持久化。

```
<Context\>
<Manager className\="org.apache.catalina.session.PersistentManager"\>
        <Store className="org.apache.catalina.session.FileStore"
               directory="xxx" />
</Manager\>
</Context\>
```

会话存储位置由 directory 参数控制，默认值为：
<TOMCAT_HOME>/work/Catalina/localhost/<your-app>。

- 如果 directory 参数提供的值与默认值不同，则不受漏洞影响。
- 如果 directory 参数没有提供，需添加参数并指定路径，路径不能为默认值。
- 如果 directory 参数值与默认值相同，需要修改路径。

4. 以上缓解措施执行完成后需要重启 tomcat 服务生效。

> ⚠ **注意：**
> 此步骤可能造成业务中断，请挑选合适时间尽快执行！

```
sudo systemctl restart tomcat
```

# TencentOS Server 关于 CUPS 远程代码执行漏洞的说明

最近更新时间：2024-11-13 16:56:42

近日，CVE 官网披露了 1 例 **CUPS**（Common UNIX Printing System）**系列**高风险组合漏洞，利用链涉及多个漏洞编号，分别为 CVE-2024-47076、CVE-2024-47175、CVE-2024-47176、CVE-2024-47177、CVE-2024-47850。此漏洞组合利用可导致未经身份验证的远程攻击者可以执行任意代码，对服务器安全构成严重威胁。
接到漏洞情报后，腾讯云开发团队第一时间对该漏洞进行了深入分析，并迅速推出修复方案。目前，TencentOS 已及时修复 CUPS 远程代码执行漏洞，为用户提供了安全可靠的操作系统环境。

## 一、漏洞概述

CUPS 是一个广泛用于 Linux 和其他类 UNIX 操作系统的开源打印系统，它使用 Internet Printing Protocol (IPP) 来实现本地和网络打印机的打印功能。
当 cups-browsed 服务启用时，未经身份验证的远程攻击者可通过向目标系统的 631 端口发送 UDP 数据包进行利用，通过构造恶意的 IPP URL 替换现有的打印机（或安装新的打印机），从而导致当服务器在启动打印作业时执行任意代码。

| 漏洞概述 | | | | | |
|---|---|---|---|---|---|
| 漏洞编号 | CVE-2024-47176 | CVE-2024-47175 | CVE-2024-47076 | CVE-2024-47177 | CVE-2024-47850 |
| 风险级别 | 高危 | 高危 | 高危 | 中危 | 高危 |
| CVSS3.1分数 | 8.4 | 8.6 | 8.6 | 6.1 | 7.5 |
| 漏洞概况 | **组件说明：**CUPS〔Common UNIX Printing System〕是一个开源的打印系统，广泛用于Linux和其他类UNIX操作系统。CUPS使用Internet Printing Protocol (IPP) 来实现本地和网络打印机的打印功能。<br>**漏洞情况：**CUPS 被披露其存在远程代码执行漏洞，利用链涉及多个漏洞编号，分别为CVE-2024-47176, CVE-2024-47175, CVE-2024-47076, CVE-2024-47177，CVE-2024-47850。可导致未经身份验证的远程攻击者执行任意代码等危害。<br>**利用条件：**CUPS 打印系统存在远程代码执行漏洞，当 cups-browsed 服务启用时，未经身份验证的远程攻击者可通过向目标系统的 631 端口发送 UDP 数据包进行利用，通过构造恶意的 IPP URL 替换现有的打印机〔或安装新的打印机〕，从而导致当服务器在启动打印作业时执行任意代码。 | | | | |
| 公开时间 | 2024/9/26 | POC状态 | 已公开 | EXP状态 | 已公开 |
| 影响组件版本 | 涉及的操作系统版本：TencentOS Server 2.x 、TencentOS Server 3.x、TencentOS Server 4.x<br>TS2：cups-filters < 1.0.35-29.tl2.3<br>TS3：cups-filters < 1.20.0-35.tl3<br>TS4：cups-filters < 1.28.16-10.tl4；cups <2.4.6-7.tl4 | | | | |

## 二、影响范围与自查方式

受此安全漏洞影响的操作系统版本包括：TencentOS Server 2、TencentOS Server 3、TencentOS Server 4。
影响的软件包版本范围包括：

- TencentOS Server 2：cups-filters < 1.0.35-29.tl2.3

- TencentOS Server 3：cups-filters < 1.20.0-35.tl3
- TencentOS Server 4：cups-filters < 1.28.16-10.tl4，cups <2.4.6-7.tl4

### 自查影响方式

由于 CUPS 系列漏洞攻击入口为 cups-browsed 组件，因此可以执行如下命令验证各自名下服务器 cups-browsed 的开放状态，从而判断自身是否受到影响：

```
sudo systemctl status cups-browsed
```

如果显示找不到单元或者 `Active: inactive (dead)` ，表示系统不受漏洞影响。如果服务状态为 `running` 或 `enabled` ，表示系统易受攻击，需要采取措施进行缓解/修复。

## 三、规避与修复方案

接到漏洞情报后，腾讯云开发团队第一时间对该漏洞进行了深入分析，并迅速推出修复方案。目前，TencentOS 已及时修复 CUPS 远程代码执行漏洞。

### 临时缓解措施

对于启用了 CUPS 服务的机器，建议禁用 cups-browsed 组件，或者通过防火墙限制对 UDP 631 端口的访问，仅允许可信的网络设备连接。执行命令如下：

```
sudo systemctl stop cups-browsed.service
sudo systemctl disable cups-browsed.service
```

### 修复方案

- TencentOS Server 2

  ```
  dnf update -y cups-filters
  ```

- TencentOS Server 3

  ```
  dnf update -y cups-filters
  ```

- TencentOS Server 4

  ```
  dnf update -y cups-filters cups
  ```

修复后的版本如下：

- TencentOS Server 2：cups-filters-1.0.35-29.tl2.3
- TencentOS Server 3：cups-filters-1.20.0-35.tl3
- TencentOS Server 4：cups-filters-1.28.16-10.tl4，cups-2.4.6-7.tl4

> **注意：**
> 对于使用 TencentOS 的用户，建议及时更新系统，以确保系统的安全性。

TencentOS 团队将持续关注安全动态，不断加强系统的安全防护能力，为用户的业务保驾护航。