GUIDE

Debian 13.5 'Trixie' Point Release: Critical Security & Stability Updates

> 🚨 **CRITICAL** — Security fix. Upgrade immediately.

> **Version:** 13.5 | **Released:** 2026-05-16 | **Upgrade from:** 13.4

Release at a Glance

The Debian project has rolled out its 13.5 'Trixie' point release, a crucial update focusing on security and stability. This isn't a feature release, but rather a vital maintenance update for the current stable branch.

Here's the TL;DR for developers:

- **Critical Security Patches:** Over 100 security fixes, including high-impact vulnerabilities in `apache2`, `aiohttp`, and `Bubblewrap`.
- **Stability Improvements:** Addresses 144 bug corrections, enhancing the overall reliability of the 'Trixie' distribution.
- **Package Removal:** The `dav4tbsync` package has been removed due to dependency changes or superseded functionality.
- **Immediate Upgrade Recommended:** All Debian 13 'Trixie' users, especially those managing servers or internet-facing systems, should prioritize this upgrade.

Security Fixes (CVE-xxxx-xxxx)

This 13.5 point release is heavily focused on shoring up the security posture of Debian 'Trixie', incorporating 103 security fixes across various packages. These patches address a range of vulnerabilities, from privilege escalation to remote code execution risks.

Key Security Patches:

- **apache2:** A series of critical fixes for the Apache HTTP Server.
  - **CVE-2026-23918:** Addresses a use-after-free vulnerability that could lead to denial of service or potentially arbitrary code execution.
  - **CVE-2026-24072:** Fixes a privilege escalation issue, preventing attackers from gaining elevated access.
  - **CVE-2026-29169, CVE-2026-33007:** Corrects NULL pointer dereference issues, mitigating potential crashes and denial of service.
  - **CVE-2026-33006:** Resolves an authentication bypass vulnerability, preventing unauthorized access.
- **aiohttp:**
  - **CVE-2026-34525:** Fixes an issue where multiple Host headers were allowed, which could be exploited in certain request smuggling or cache poisoning scenarios.
- **Bubblewrap:**
  - Addresses a privilege escalation issue, enhancing the security of sandboxed applications.
- **Git v2.13.5:**
  - Includes a forward-ported fix for 'ssh://...' URL handling, mitigating potential command injection or unexpected behavior when processing malicious URLs.
- **Undisclosed Code Execution Fix:**
  - A fix for a code execution issue has been applied, though the specific package details were not provided in the release evidence. This highlights the breadth of the security audit.

🧠 **Important:** These security fixes are paramount for maintaining the integrity and availability of your Debian systems. Exploitation of such vulnerabilities can lead to data breaches, system compromise, or service disruption.

Bug Patches

Beyond the critical security updates, Debian 13.5 'Trixie' also incorporates a significant number of stability improvements. The release includes **144 bug corrections** that address various issues encountered in the 13.x series. While specific details for each bug fix are not individually enumerated in the high-level release notes, these corrections contribute to:

- Improved system reliability and uptime.
- Resolution of minor regressions and unexpected behavior.
- Better compatibility with updated hardware and software components.

These general stability enhancements are crucial for long-term operational integrity, ensuring that 'Trixie' remains a robust and dependable operating system for all use cases.

Breaking Changes and Removed APIs

Point releases typically aim for maximum compatibility, but sometimes a package must be removed due to upstream changes, lack of maintenance, or dependency conflicts. Debian 13.5 includes one notable package removal.

`dav4tbsync` Package Removal

The `dav4tbsync` package has been removed from the Debian 'Trixie' distribution.

Reason for Removal: The removal is attributed to "changes in dependencies or superseded functionality." This often occurs when a package relies on libraries that are no longer available or have undergone significant, incompatible changes, or when its functionality has been absorbed into other, more actively maintained tools.

Impact: Users who rely on `dav4tbsync` for WebDAV synchronization will find it no longer available in the official repositories. They will need to:

1. **Identify Alternatives:** Seek alternative tools or methods for WebDAV synchronization.
2. **Migrate Data/Workflows:** Adjust their workflows to use the new solution.

3. **Consider Manual Installation:** If absolutely necessary and an alternative is not viable, users might consider compiling and installing `dav4tbsync` manually from source, though this is generally not recommended for stability and security reasons in a production environment.

For most users, this change will have minimal impact unless `dav4tbsync` was an integral part of their specific setup.

Overall Impact on System Stability and Security

The Debian 13.5 'Trixie' point release delivers a substantial boost to both the security and stability of the distribution. The sheer volume of security fixes (103 CVEs) indicates a thorough review and remediation process, addressing vulnerabilities that could have severe consequences if exploited.

Security Enhancement: The patches for `apache2`, `aiohttp`, `Bubblewrap`, and `Git` are particularly noteworthy, as these are widely used components in server environments and developer toolchains. By patching these, Debian significantly reduces the attack surface for many common deployment scenarios. For instance, fixing privilege escalation in `Bubblewrap` enhances the security of containerized or sandboxed applications, while `apache2` fixes protect web servers from critical vulnerabilities like use-after-free and authentication bypass.

Stability Improvement: The 144 bug corrections, while less dramatic than security fixes, are equally important for the day-to-day operation of systems. They iron out kinks, improve robustness, and ensure a smoother, more predictable user experience. This cumulative effect leads to a more reliable operating system that requires less troubleshooting and maintenance.

Who Should Upgrade: Given the critical nature of the security fixes, **all users running Debian 13 'Trixie' are strongly advised to upgrade immediately.** This is especially true for:

- **Servers and Internet-facing Systems:** These are the primary targets for exploitation of the types of vulnerabilities patched in this release.
- **Development Workstations:** To protect against supply chain attacks and ensure the security of development environments.
- **Any System Handling Sensitive Data:** To minimize the risk of data compromise.

This release reinforces Debian's commitment to providing a secure and stable foundation, making it an essential update for maintaining a healthy and protected system.

How to Upgrade

Upgrading to Debian 13.5 'Trixie' is a standard procedure for Debian users and is highly recommended due to the critical security and stability updates.

Prerequisites:

- Ensure your system is connected to the internet.
- It's always a good practice to back up important data before any system-wide upgrade.

Upgrade Steps:

1. **Update Package Lists:** First, refresh your local package index to ensure you have the latest information about available packages and their versions from the Debian repositories.

```
sudo apt update
```

1. **Perform the Upgrade:** Next, perform a full system upgrade. This command will install new versions of packages that are currently installed on your system and will also install any new dependencies.

```
sudo apt upgrade
```

```
If `apt upgrade` suggests additional packages to remove or install (e.g., due to dependency changes or kernel updates), you might consider using `apt full-upgrade` for a more comprehensive update. This command is more aggressive and will handle dependency changes by removing obsolete packages and installing new ones as needed.
```

```
sudo apt full-upgrade
```

1. **Clean Up (Optional but Recommended):** After the upgrade, you can remove any no-longer-needed packages and clean up the `apt` cache to free up disk space.

```
sudo apt autoremove
sudo apt clean
```

1. **Reboot (If Necessary):** If the upgrade included updates to the kernel or other critical system components (like `systemd`), a reboot is required for the changes to take full effect.

```
sudo reboot
```

After these steps, your Debian 13 'Trixie' system will be running version 13.5, incorporating all the latest security patches and stability improvements.