Security vulnerability alert for Parallels Desktop running on Intel Macs

- Parallels Desktop for Mac Business Edition
- Parallels Desktop for Mac Standard Edition
- Parallels Desktop for Mac Enterprise Edition
- Parallels Desktop for Mac Pro Edition

On 20 February 2025, an independent security researcher published an exploit that affects Intel Mac users on the latest versions of Parallels Desktop.

Exploit nature: an attacker who has access to the Mac, but doesn't have root privileges can acquire ones by exploiting the Parallels Desktop macOS VM creation routine on Intel Mac computers.

Upon discovery, Parallels took the following actions:

- **Immediate Mitigation:** Parallels has released hotfixes to address the issue in the latest versions of Parallels Desktop.
- **Inform Customers:** informed customers through various means.
- **Prevention:** postmortem activities were scheduled shortly after the release.

Who can be affected by the exploit?

Only users who create a new macOS virtual machine on a Mac with an Intel processor.

If you run Parallels Desktop on a Mac with an Apple silicon chip or you don't create new macOS virtual machines, you're not affected by the exploit. All the customers can **continue to use existing** Windows, Linux, or macOS virtual machines without any issues. If you use Parallels Desktop App Store Edition, you're not affected by the exploit, either.

Are there any recommendations from Parallels?

We recommend the following actions to ensure your continued security:

The issue has been addressed in Parallels Desktop 20.2.2 and 19.4.2 builds. We recommend you to update Parallels Desktop to the latest version by clicking the Parallels icon in the Mac menu bar > Check for updates.

Note: all users can continue to use existing Windows, Linux, or macOS virtual machines without any issues.

Is it fixed?

Parallels has released hotfixes to address the issue in the latest versions of Parallels Desktop:

- **27 February** for Parallels Desktop 20.2.2
- **March 6** for Parallels Desktop 19.4.2

Our Commitment

We are dedicated to maintaining high security standards. Our team continuously monitors potential threats and provides updates as necessary. If you believe you have found a security issue in Parallels Desktop, visit KB article: How to Submit a Responsible Disclosure .

We apologize for any inconvenience this may have caused and appreciate your understanding and cooperation.
