



Mitigate ZDI-CAN-13543 in Parallels Desktop 16 and older

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

During the Pwn2Own 2021 hackathon, the ZDI-CAN-13543 vulnerability has been found: malicious software running in a virtual machine (VM) can potentially access macOS files that are shared in a default configuration with Parallels Tools installed.

By default, Parallels Desktop shares files and folders between the Mac and a VM, so users can easily open macOS files from applications running in a virtual machine and save documents to Mac. Learn more in [KB 6912](#).

This functionality exposes the user home folder to the VM. This folder may contain configuration files, cache from different applications, etc., that malicious software can access.

Affected versions

Parallels Desktop 16 for Mac and older.

Not affected versions

Parallels Desktop 17 for Mac and newer versions are not affected. The entire home folder is no longer shared with a VM by default, only selected folders, like Desktop, Documents, Downloads, etc.

Mitigations

If you don't plan to run untrusted code in the VM, it is recommended to follow common security practices.

If you run untrusted code in the VM and you want to isolate the VM from Mac, then one of the following options can be used:

Note: Implementing one of these steps will result in reduced functionality, causing file duplications and inconvenience when using documents across VM and Mac.

1. Disable shared folders as described in [KB 6912](#). Shared Profile functionality will be disabled as well, and you will no longer be able to open Mac files in the VM or save files to Mac. Learn more in [KB 6912](#).
 2. Alternatively, isolate the VM from Mac as described in [KB 112942](#). After isolating, folders, files, applications, and external drives are not shared between two operating systems. In general, it becomes impossible for a VM to access any information on your Mac. Isolating a virtual machine provides the highest level of security.
-