Parallels Statement on Apache CVE-2021-44228

- Parallels Remote Application Server
- Parallels Desktop for Chrome OS Enterprise and Education Edition
- Parallels Access
- Parallels Device Management
- Parallels Desktop for Mac App Store Edition
- Parallels Toolbox Business Edition
- Parallels Desktop for Mac Pro Edition
- Parallels Toolbox
- Parallels Desktop for Mac Business Edition
- Parallels Desktop for Mac Standard Edition
- Parallels Transporter

Parallels is aware of the security vulnerability CVE-2021-44228 affecting Apache Log4j2 which, if exploited, allows an attacker who is able to control log messages or log message parameters to execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Security vulnerability description: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Please be advised that Parallels products **are not** affected by CVE-2021-44228 (Log4Shell) since it doesn't use the Log4j library.

Parallels did investigate the potential impact on Parallels products. Please find the present status of every product below:

Product	Status
Parallels RAS	Not affected
Parallels Desktop	Not affected
Parallels Access	Not affected (all platforms)
Parallels Toolbox	Not affected (all platforms)
Parallels Device Management	Not affected
Parallels Client	Not affected (all platforms)
Parallels Transporter	Not affected (all platforms)