

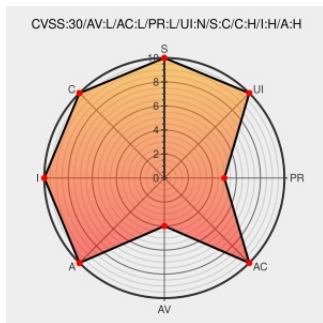


CVE-2020-17392

Published on: 08/25/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:30 PM UTC

CVE-2020-17392

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Parallels Desktop](#) from [Parallels](#) contain the following vulnerability:

This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.3-47255. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handler for `HOST_IOCTL_SET_KERNEL_SYMBOLS` in the

`prl_hypervisor` kext. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the kernel. Was ZDI-CAN-10519.

CVE-2020-17392 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Parallels - Desktop** version **15.1.3-47255**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References						
Description		Tags	Link			
KB Parallels: Parallels Desktop Security Updates		Vendor Advisory kb.parallels.com text/html	MISC kb.parallels.com/en/125013			
ZDI-20-1010 Zero Day Initiative		Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	Z MISC www.zerodayinitiative.com/advisories/ZDI-20-1010/			
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Parallels	Parallels Desktop	All	All	All	All
Application	Parallels	Parallels Desktop	All	All	All	All
cpe:2.3:a:parallels:parallels_desktop:*:*:*:*:macos:*:*:						
cpe:2.3:a:parallels:parallels_desktop:*:*:*:*:macos:*:*:						
Discovery Credit						
Reno Robert						

← Previous ID

Next ID →