

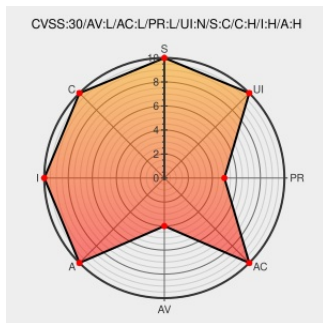


CVE-2021-31425

Published on: 04/29/2021 12:00:00 AM UTC

Last Modified on: 05/07/2021 06:34:00 PM UTC

CVE-2021-31425

[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 16.1.2-49151. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Parallels Tools component. The issue results from the

lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel on the target guest system. Was ZDI-CAN-12790.

CVE-2021-31425 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Parallels - Desktop** version **16.1.2-49151**

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: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
KB Parallels: Parallels Desktop Security Updates	kb.parallels.com text/html	MISC kb.parallels.com/en/125013
ZDI-21-432 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-432/

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	16.1.2-49151	All	All	All

cpe:2.3:a:parallels:parallels_desktop:16.1.2-49151:*****:

Discovery Credit

grigoritchy

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31425 : This vulnerability allows local attackers to escalate privileges on affected installations of Para... twitter.com/i/web/status/1...	2021-04-29 16:36:43
/r/netcve	CVE-2021-31425	2021-04-29 16:41:59

[← Previous ID](#)[Next ID →](#)