CVE-2021-31422

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

Last Modified on: 05/10/2021 01:49:00 PM UTC

CVE-2021-31422

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 16.1.1-49141. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the e1000e virtual device. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12527.

CVE-2021-31422 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Parallels** - **Desktop** version **16.1.1-49141**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
KB Parallels: Parallels Desktop Security Updates	kb.parallels.com text/html	MISC kb.parallels.com/en/125013
ZDI-21-430 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-430/

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	16.1.1-49141	All	All	All

cpe:2.3:a:parallels:parallels_desktop:16.1.1-49141:*:*:*:*:*:*:*:

Discovery Credit

Anonymous

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31422 : This vulnerability allows local attackers to escalate privileges on affected installations of Para… twitter.com/i/web/status/1…	2021-04-29 16:35:40
/r/netcve	CVE-2021-31422	2021-04-29 16:41:57

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report