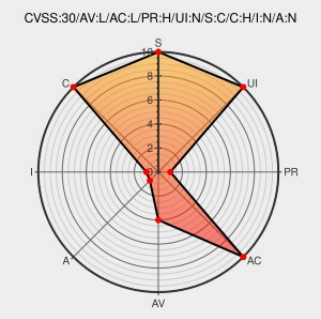
CVE-2021-31423

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

Last Modified on: 05/07/2021 02:24:00 AM UTC

CVE-2021-31423

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 disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. 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 Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12528.

CVE-2021-31423 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Parallels** - **Desktop** version **15.1.5-47309**

CVSS3 Score: 6 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
KB Parallels: Parallels Desktop Security Updates	kb.parallels.com text/html	MISC kb.parallels.com/en/125013
ZDI-21-431 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-431/

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	15.1.5-47309	All	All	All

cpe:2.3:a:parallels:parallels_desktop:15.1.5-47309:*:*:*:*:*:*:*:

Discovery Credit

Anonymous

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31423 : This vulnerability allows local attackers to disclose sensitive information on affected installati… twitter.com/i/web/status/1…	2021-04-29 16:36:01
/r/netcve	CVE-2021-31423	2021-04-29 16:41:58

← Previous ID

Next ID→