

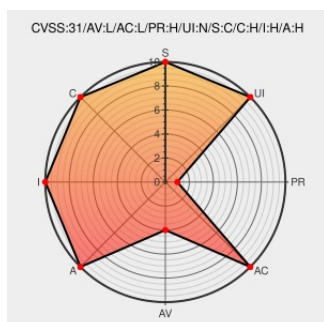


CVE-2020-14628

Published on: 07/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:01 PM UTC

CVE-2020-14628

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

Certain versions of [Leap](#) from [Opensuse](#) contain the following vulnerability:

Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise

Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: The CVE-2020-14628 is applicable to Windows VM only. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).

CVE-2020-14628 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Oracle Corporation](#) - **VM VirtualBox** version < **5.2.44**

Affected Vendor/Software: [Oracle Corporation](#) - **VM VirtualBox** version < **6.0.24**

Affected Vendor/Software: [Oracle Corporation](#) - **VM VirtualBox** version < **6.1.12**

CVSS3 Score: **8.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	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

LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References		
Description	Tags	Link
Oracle Critical Patch Update Advisory - July 2020	Vendor Advisory www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujul2020.html
VirtualBox: Multiple vulnerabilities (GLSA 202101-09) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-202101-09
ZDI-20-886 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-886/
[security-announce] openSUSE-SU-2020:1486-1: moderate: Security update f	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1486
[security-announce] openSUSE-SU-2020:1511-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1511

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.

Related QID Numbers
690525 Free Berkeley Software Distribution (FreeBSD) Security Update for virtualbox (1e7b316b-c6a8-11ea-a7d5-001999f8d30b)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All
Application	Oracle	Vm Virtualbox	All	All	All	All

cpe:2.3:o:opensuse:leap:15.1:*****:

cpe:2.3:o:opensuse:leap:15.1:*****:
cpe:2.3:o:opensuse:leap:15.2:*****:
cpe:2.3:o:opensuse:leap:15.1:*****:
cpe:2.3:o:opensuse:leap:15.2:*****:
cpe:2.3:a:oracle:vm_virtualbox:*****:
cpe:2.3:a:oracle:vm_virtualbox:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)