

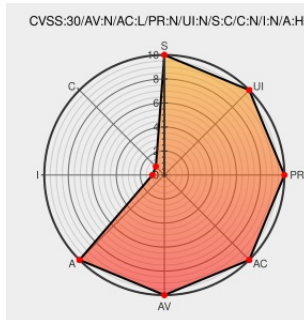


CVE-2020-2959

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-2959

[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 5.2.40, prior to 6.0.20 and prior to 6.1.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via MLD 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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).

CVE-2020-2959 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 < 5.2.40

Affected Vendor/Software: Oracle Corporation - VM VirtualBox version < 6.0.20

Affected Vendor/Software: Oracle Corporation - VM VirtualBox version < 6.1.6

CVSS3 Score: **8.6 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact				
NONE	NONE	PARTIAL				
CVE References						
Description	Tags	Link				
VirtualBox: Multiple vulnerabilities (GLSA 202101-09) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-202101-09				
Oracle Critical Patch Update Advisory - April 2020	Vendor Advisory www.oracle.com text/html	 MISC www.oracle.com/security-alerts/cpuapr2020.html				
[security-announce] openSUSE-SU-2020:0925-1: moderate: Security update f	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0925				
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
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	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:a:oracle:vm_virtualbox:*****:.*						
cpe:2.3:a:oracle:vm_virtualbox:*****:.*						
No vendor comments have been submitted for this CVE						
← Previous ID Next ID →						

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 registered 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](#)