



CVE-2017-3316

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3316
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-27 22:59:00 UTC
Updated	2017-09-02 01:29:00 UTC
Description	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: GUI). Supported versions that

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Vm Virtualbox	5.0.30	All	All	All
Application	Oracle	Vm Virtualbox	5.1.12	All	All	All
Application	Oracle	Vm Virtualbox	5.0.30	All	All	All
Application	Oracle	Vm Virtualbox	5.1.12	All	All	All

References

Reference
Oracle Virtualization Lets Remote and Local Users Access and Modify Data and Deny Service, Local Users Modify Data, and Remote Authent
Oracle VM VirtualBox CVE-2017-3316 Remote Security Vulnerability
Oracle Critical Patch Update - January 2017
VirtualBox: Multiple vulnerabilities (GLSA 201702-08) — Gentoo Security
Oracle VM VirtualBox < 5.0.32 / < 5.1.14 - Local Privilege Escalation - Linux local Exploit
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

710538 Gentoo Linux VirtualBox Multiple Vulnerabilities (GLSA 201702-08)

© [CVE.report](#) 2026 |

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 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)