



CVE-2008-3431

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

Summary

CVE	CVE-2008-3431
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-05 19:41:00 UTC
Updated	2026-04-22 14:12:18 UTC
Description	The VBoxDrvNtDeviceControl function in VBoxDrv.sys in Sun xVM VirtualBox before 1.6.4 uses the METHOD_NEITHER c

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.053780000 probability, percentile 0.901300000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.2		AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Oracle
Product	VirtualBox
Name	Oracle VirtualBox Insufficient Input Validation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2008-3431

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Virtualbox	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

Sun xVM VirtualBox < 1.6.4 - Privilege Escalation (PoC) - Multiple dos Exploit

www.cisa.gov/known-exploited-vulnerabilities-catalog

Changelog - VirtualBox

IBM X-Force Exchange

SecurityReason - Sun xVM VirtualBox Privilege Escalation Vulnerability

SecurityFocus

Core Security Technologies

Sun xVM VirtualBox "VBoxDrv.sys" IOCTL Privilege Escalation Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Sun xVM VirtualBox Lets Local Users Gain Full Privileges - SecurityTracker

sunsolve.sun.com/search/document.do

Sun xVM VirtualBox 'VBoxDrv.sys' Local Privilege Escalation Vulnerability

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-03T00:00:00.000Z	CVE-2008-3431 added to CISA KEV

Legacy QID Mappings

[376503](#) Sun Virtualized Manager (VM) VirtualBox Privilege Escalation Vulnerability

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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