

CVE-2008-3431

Oracle VirtualBox Insufficient Input Validation Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

The VBoxDrvNtDeviceControl function in VBoxDrv.sys in Sun xVM VirtualBox before 1.6.4 uses the METHOD_NEITHER communication method for IOCTLs and does not properly validate a buffer associated with the Irp object, which allows local users to gain privileges by opening the \\.\VBoxDrv device and calling DeviceIoControl to send a crafted kernel address.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.069 94th percentile · FIRST	CISA DEADLINE Mar 24, 2022 KEV since 2022 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.069 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
virtualbox	< 1.6.4	1.6.4	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2008-3431

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2008-3417

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2008-3431

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.