



# CVE-2023-5090

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

## Summary

<b>CVE</b>	CVE-2023-5090
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-06 11:15:00 UTC
<b>Updated</b>	2023-11-14 17:01:00 UTC
<b>Description</b>	A flaw was found in KVM. An improper check in svm_set_x2apic_msr_interception() may allow direct access to host x2apic

## Risk And Classification

**Problem Types:** CWE-755

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	6.6	rc1	All	All
Operating System	Linux	Linux Kernel	6.6	rc2	All	All
Operating System	Linux	Linux Kernel	6.6	rc3	All	All
Operating System	Linux	Linux Kernel	6.6	rc4	All	All
Operating System	Linux	Linux Kernel	6.6	rc5	All	All
Operating System	Linux	Linux Kernel	6.6	rc6	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

## References

### Reference

[cve-details](#)

[2248122 – \(CVE-2023-5090\) CVE-2023-5090 kernel: KVM: SVM: improper check in svm\\_set\\_x2apic\\_msr\\_interception allows direct access to](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160978](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12874)

[160982](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12911)

[160985](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12910)

[161237](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13043)

[199929](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6497-1)

[199933](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6502-1)

[199938](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6503-1)

[199952](#) Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-6502-2)

[199957](#) Ubuntu Security Notification for Linux kernel (StarFive) Vulnerabilities (USN-6520-1)

[199958](#) Ubuntu Security Notification for Linux kernel (NVIDIA) Vulnerabilities (USN-6502-3)

[199973](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6502-4)

[199982](#) Ubuntu Security Notification for Linux kernel (GCP) Vulnerability (USN-6537-1)

[356908](#) Amazon Linux Security Advisory for kernel : ALAS2023-2023-430

[356919](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-026

[356921](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-022

[356922](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-023

[356923](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-024

[356924](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-025

[356925](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-021

[6140012](#) AWS Bottlerocket Security Update for kernel (GHSA-h793-mm5x-7p69)

[6140051](#) AWS Bottlerocket Security Update for kernel (GHSA-h793-mm5x-7p69)

© [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](#).

