



# CVE-2022-2153

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

## Summary

<b>CVE</b>	CVE-2022-2153
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-31 16:15:00 UTC
<b>Updated</b>	2022-11-21 19:45:00 UTC
<b>Description</b>	A flaw was found in the Linux kernel's KVM when attempting to set a SynIC IRQ. This issue makes it possible for a misbeh

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 3131-1] linux security update	MLIST	<a href="#">lists...</a>
KVM: x86: Forbid VMM to set SYNIC/STIMER MSRs when SynIC wasn't activ... · torvalds/linux@b1e34d3 · GitHub	MISC	<a href="#">github</a>
KVM: x86: Check lapic_in_kernel() before attempting to set a SynIC irq · torvalds/linux@7ec37d1 · GitHub	MISC	<a href="#">github</a>
[SECURITY] [DLA 3173-1] linux-5.10 security update	MLIST	<a href="#">lists...</a>
oss-security - CVE-2022-2153: Linux Kernel: x86/kvm: NULL pointer dereference in kvm_irq_delivery_to_apic_fast	MISC	<a href="#">www</a>
KVM: x86: Avoid theoretical NULL pointer dereference in kvm_irq_deliv... · torvalds/linux@00b5f37 · GitHub	MISC	<a href="#">github</a>
2069736 - (CVE-2022-2153) CVE-2022-2153 kernel: KVM: NULL pointer dereference in kvm_irq_delivery_to_apic_fast()	MISC	<a href="#">bugz</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160043](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9709)

[160045](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9710)

[179388](#) Debian Security Update for linux (CVE-2022-2153)

[180282](#) Debian Security Update for linux (DLA 3065-1)

[180605](#) Debian Security Update for linux (DSA 5173-1)

[181091](#) Debian Security Update for linux (DLA 3131-1)

[181190](#) Debian Security Update for linux-5.10 (DLA 3173-1)

[199029](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5728-1)

[199030](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5727-1)

[199036](#) Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5727-2)

[199037](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5728-2)

[199051](#) Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5728-3)

[199072](#) Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5774-1)

[354053](#) Amazon Linux Security Advisory for kernel : ALAS2-2022-1838

[354071](#) Amazon Linux Security Advisory for kernel : ALAS-2022-1636

[354075](#) Amazon Linux Security Advisory for kernel : ALAS2-2022-1852

[354081](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-036

[354084](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-020

[377117](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)

[377766](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0049)

[377871](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0001)

[6140266](#) AWS Bottlerocket Security Update for kernel (GHSA-3rg2-x5gq-4xgg)

[672114](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2292)

[672139](#) EulerOS Security Update for kernel (EulerOS-SA-2022-2428)

672158 EulerOS Security Update for kernel (EulerOS-SA-2022-2415)
752813 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3930-1)
752839 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3929-1)
752880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4053-1)
752889 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3897-1)
752911 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)
752913 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4072-1)
752944 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4273-1)
752959 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4272-1)
753038 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4573-1)
753039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4574-1)
753051 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4589-1)
753060 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4615-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
903738 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10801)
903804 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10794)
904088 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10801-1)
904148 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10794-1)
905932 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10801-2)
906364 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10794-2)

© [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](#).

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