



CVE-2022-4139

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

Summary

CVE	CVE-2022-4139
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-27 18:15:00 UTC
Updated	2023-05-12 13:28:00 UTC
Description	An incorrect TLB flush issue was found in the Linux kernel's GPU i915 kernel driver, potentially leading to random memory

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	6.1	-	All	All
Operating System	Linux	Linux Kernel	6.1	rc1	All	All
Operating System	Linux	Linux Kernel	6.1	rc2	All	All
Operating System	Linux	Linux Kernel	6.1	rc3	All	All
Operating System	Linux	Linux Kernel	6.1	rc4	All	All
Operating System	Linux	Linux Kernel	6.1	rc5	All	All
Operating System	Linux	Linux Kernel	6.1	rc6	All	All

References

Reference	Source	Link
CVE-2022-4139 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	secu
2147572 – (CVE-2022-4139) CVE-2022-4139 kernel: i915: Incorrect GPU TLB flush can lead to random memory access	MISC	bugzi
oss-security - Security sensitive bug in the i915 kernel driver (CVE-2022-4139)	MISC	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160392](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0101)

[160423](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0334)

[160457](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12121)

[160459](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12116)

[160460](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12120)

[160462](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12119)

[181371](#) Debian Security Update for linux (CVE-2022-4139)

[181440](#) Debian Security Update for linux-5.10 (DLA 3244-1)

[199156](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5859-1)

[199209](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5912-1)

[199211](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5911-1)

[199212](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5917-1)

[199220](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5929-1)

[199223](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5935-1)

[199224](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5934-1)

[199226](#) Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5939-1)

[199227](#) Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5938-1)

[199229](#) Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-5941-1)

[199230](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5940-1)

[199238](#) Ubuntu Security Notification for Linux kernel (KVM) Vulnerabilities (USN-5950-1)

[199239](#) Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5951-1)

[199243](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5962-1)

[199276](#) Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6000-1)

[199352](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerability (USN-6089-1)

[199380](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6124-1)

[241047](#) Red Hat Update for kpatch-patch (RHSA-2023:0123)

241049 Red Hat Update for kernel (RHSA-2023:0101)
241051 Red Hat Update for kernel-rt (RHSA-2023:0114)
241095 Red Hat Update for kernel (RHSA-2023:0334)
241096 Red Hat Update for kernel-rt (RHSA-2023:0300)
241101 Red Hat Update for kpatch-patch (RHSA-2023:0348)
241127 Red Hat Update for kpatch-patch (RHSA-2023:0441)
241128 Red Hat Update for kernel (RHSA-2023:0440)
241144 Red Hat Update for kpatch-patch (RHSA-2023:0499)
241147 Red Hat Update for kernel (RHSA-2023:0496)
241149 Red Hat Update for kernel (RHSA-2023:0512)
241150 Red Hat Update for kernel-rt (RHSA-2023:0531)
241151 Red Hat Update for kpatch-patch (RHSA-2023:0536)
241152 Red Hat Update for kernel-rt (RHSA-2023:0526)
283382 Fedora Security Update for kernel (FEDORA-2022-24041b1667)
283383 Fedora Security Update for kernel (FEDORA-2022-b36cd53dca)
283390 Fedora Security Update for kernel (FEDORA-2022-e4460c41bc)
355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
753015 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15 SP3) (SUSE-SU-2022:4544-1)
753016 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP2) (SUSE-SU-2022:4587-1)
753017 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 4 for SLE 15 SP4) (SUSE-SU-2022:4560-1)
753020 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4585-1)
753021 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:4528-1)
753022 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 20 for SLE 15 SP3) (SUSE-SU-2022:4551-1)
753023 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 5 for SLE 15 SP4) (SUSE-SU-2022:4542-1)
753029 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 25 for SLE 15 SP3) (SUSE-SU-2022:4517-1)
753031 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 31 for SLE 15 SP2) (SUSE-SU-2022:4515-1)
753032 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15 SP2) (SUSE-SU-2022:4512-1)

753032 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 27 for SLE 15 SP2) (SUSE-SU-2022:4513-1)
753033 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 1 for SLE 15 SP4) (SUSE-SU-2022:4518-1)
753034 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4504-1)
753035 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP2) (SUSE-SU-2022:4534-1)
753037 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP2) (SUSE-SU-2022:4580-1)
753040 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 12 for SLE 15 SP3) (SUSE-SU-2022:4562-1)
753041 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP3) (SUSE-SU-2022:4516-1)
753043 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP3) (SUSE-SU-2022:4572-1)
753044 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP4) (SUSE-SU-2022:4559-1)
753045 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4503-1)
753048 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 18 for SLE 15 SP3) (SUSE-SU-2022:4569-1)
753050 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15 SP3) (SUSE-SU-2022:4543-1)
753051 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4589-1)
753061 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4616-1)
753062 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4613-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
905399 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13243)
905401 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13247)
905963 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13243-2)
906306 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13247-2)
906573 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13243-4)
906612 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (13247-4)
940879 AlmaLinux Security Update for kernel (ALSA-2023:0101)
940881 AlmaLinux Security Update for kernel-rt (ALSA-2023:0114)
940904 AlmaLinux Security Update for kernel (ALSA-2023:0334)
940910 AlmaLinux Security Update for kernel-rt (ALSA-2023:0300)
960498 Rocky Linux Security Update for kernel (RLSA-2023:0101)
960503 Rocky Linux Security Update for kernel-rt (RLSA-2023:0300)
960509 Rocky Linux Security Update for kernel-rt (RLSA-2023:0114)

© [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](#)