



CVE-2022-36123

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

Summary

CVE	CVE-2022-36123
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-29 14:15:00 UTC
Updated	2022-09-04 19:29:00 UTC
Description	The Linux kernel before 5.18.13 lacks a certain clear operation for the block starting symbol (.bss). This allows Xen PV gue

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference
security/SICK-2022-128.md at master · sickcodes/security · GitHub
CVE-2022-36123 - A vulnerability in Linux kernel mainline v5.18-rc1 through v5.19-rc6 does not clear statically allocated variables in the block
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.18.13

[x86/xen: Use clear_bss\(\) for Xen PV guests](#) · [torvalds/linux@96e8fc5](#) · [GitHub](#)

[CVE-2022-36123 Linux Kernel Vulnerability in NetApp Products](#) | [NetApp Product Security](#)

Merge tag 'x86_urgent_for_v5.19_rc6' of [git://git.kernel.org/pub/scm/...](#) · [torvalds/linux@74a0032](#) · [GitHub](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[183451](#) [Debian Security Update for linux \(CVE-2022-36123\)](#)

[354044](#) [Amazon Linux Security Advisory for kernel : ALAS2-2022-1833](#)

[354051](#) [Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-019](#)

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

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

[354385](#) [Amazon Linux Security Advisory for kernel : ALAS2022-2022-125](#)

[354468](#) [Amazon Linux Security Advisory for kernel : ALAS2022-2022-185](#)

[354542](#) [Amazon Linux Security Advisory for kernel : ALAS-2022-185](#)

[355199](#) [Amazon Linux Security Advisory for kernel : ALAS2023-2023-070](#)

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

[6140309](#) [AWS Bottlerocket Security Update for kernel \(GHSA-g4hw-7h5w-ccfw\)](#)

[672141](#) [EulerOS Security Update for kernel \(EulerOS-SA-2022-2441\)](#)

[672218](#) [EulerOS Security Update for kernel \(EulerOS-SA-2022-2619\)](#)

[672278](#) [EulerOS Security Update for kernel \(EulerOS-SA-2022-2686\)](#)

[672286](#) [EulerOS Security Update for kernel \(EulerOS-SA-2022-2654\)](#)

[672391](#) [EulerOS Security Update for kernel \(EulerOS-SA-2022-2767\)](#)

[902660](#) [Common Base Linux Mariner \(CBL-Mariner\) Security Update for kernel \(10457\)](#)

[902664](#) [Common Base Linux Mariner \(CBL-Mariner\) Security Update for kernel \(10451\)](#)

[904020](#) [Common Base Linux Mariner \(CBL-Mariner\) Security Update for kernel \(10457-1\)](#)

[904125](#) [Common Base Linux Mariner \(CBL-Mariner\) Security Update for kernel \(10451-1\)](#)

[906119](#) [Common Base Linux Mariner \(CBL-Mariner\) Security Update for kernel \(10457-2\)](#)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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