



CVE-2022-0995

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

Summary

CVE	CVE-2022-0995
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-25 19:15:00 UTC
Updated	2023-11-09 14:44:00 UTC
Description	An out-of-bounds (OOB) memory write flaw was found in the Linux kernel's watch_queue event notification subsystem. This

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.17	-	All	All
Operating System	Linux	Linux Kernel	5.17	rc1	All	All
Operating System	Linux	Linux Kernel	5.17	rc2	All	All
Operating System	Linux	Linux Kernel	5.17	rc3	All	All
Operating System	Linux	Linux Kernel	5.17	rc4	All	All
Operating System	Linux	Linux Kernel	5.17	rc5	All	All
Operating System	Linux	Linux Kernel	5.17	rc6	All	All
Operating System	Linux	Linux Kernel	5.17	rc7	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	Baseboard Management Controller H300e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H300s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410c	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410c Firmware	-	All	All	All

Hardware	Netapp	Baseboard Management Controller H410s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H610c	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H610c Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H610s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H610s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H615c	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H615c Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700s Firmware	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	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	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H610c	-	All	All	All
Operating System	Netapp	H610c Firmware	-	All	All	All
Hardware	Netapp	H610s	-	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	H615c	-	All	All	All
Operating System	Netapp	H615c Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All

Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source	Link	Ta
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
March 2022 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Watch Queue Out-Of-Bounds Write ≈ Packet Storm	MISC	packetstormsecurity.com	
2063786 – (CVE-2022-0995) CVE-2022-0995 kernel: kernel bug in the watch_queue subsystem	MISC	bugzilla.redhat.com	
Linux watch_queue Filter Out-Of-Bounds Write ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179230 Debian Security Update for linux (CVE-2022-0995)
282491 Fedora Security Update for kernel (FEDORA-2022-9342e59a98)
282492 Fedora Security Update for kernel (FEDORA-2022-de4474b89d)
376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)
377124 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0029)
610432 Google Pixel Android August 2022 Security Patch Missing
900783 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9151)
901275 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9152-1)
901347 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9151-1)
906197 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9151-2)
906483 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9152-2)

© 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](#)