



CVE-2022-2964

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

Summary

CVE	CVE-2022-2964
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-09 15:15:00 UTC
Updated	2023-01-20 12:58:00 UTC
Description	A flaw was found in the Linux kernel's driver for the ASIX AX88179_178A-based USB 2.0/3.0 Gigabit Ethernet Devices. The

Risk And Classification

Problem Types: CWE-119

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	5.17	-	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
Operating System	Redhat	Enterprise Linux	7.0	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	Source	Link
CVE-2022-2964 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	secu
2067482 – (CVE-2022-2964) CVE-2022-2964 kernel: memory corruption in AX88179_178A based USB ethernet device.	MISC	bugzi
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160123 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9852)
160392 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0101)
160423 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0334)
160429 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-0399)
180968 Debian Security Update for linux (CVE-2022-2964)
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)
241124 Red Hat Update for kernel-rt (RHSA-2023:0392)
241125 Red Hat Update for kernel (RHSA-2023:0399)
241126 Red Hat Update for kernel-rt (RHSA-2023:0400)
241130 Red Hat Update for kpatch-patch (RHSA-2023:0404)
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)

241252 Red Hat Update for kernel (RHSA-2023:1130)
241254 Red Hat Update for kpatch-patch (RHSA-2023:1192)
241605 Red Hat Update for kernel (RHSA-2023:0395)
241607 Red Hat Update for kpatch-patch (RHSA-2023:0396)
241668 Red Hat Update for kpatch-patch (RHSA-2023:0858)
241684 Red Hat Update for kernel (RHSA-2023:0856)
257210 CentOS Security Update for kernel (CESA-2023:0399)
378473 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)
390268 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0026)
672278 EulerOS Security Update for kernel (EulerOS-SA-2022-2686)
672286 EulerOS Security Update for kernel (EulerOS-SA-2022-2654)
672354 EulerOS Security Update for kernel (EulerOS-SA-2022-2732)
672391 EulerOS Security Update for kernel (EulerOS-SA-2022-2767)
672410 EulerOS Security Update for kernel (EulerOS-SA-2022-2796)
672711 EulerOS Security Update for kernel (EulerOS-SA-2023-1507)
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)
753016 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15 SP2) (SUSE-SU-2022:4587-1)
753021 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:4528-1)
753036 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15) (SUSE-SU-2022:4550-1)
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)
753040 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 12 for SLE 15 SP3) (SUSE-SU-2022:4562-1)

753049	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 12 SP5) (SUSE-SU-2022:4520-1)
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)
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)
960587	Rocky Linux Security Update for kernel (RLSA-2023:0334)

© [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](#)