CVE-2021-33098

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-33098
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-17 20:15:00 UTC
Updated	2021-12-14 20:18:00 UTC
Description	Improper input validation in the Intel(R) Ethernet ixgbe driver for Linux before version 3.17.3 may allow an authenticated us

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Intel	Ethernet 500 Series Controllers Driver	All	All	All	All
Hardware	Intel	Ethernet Connection X540	-	All	All	All
Hardware	Intel	Ethernet Connection X550	-	All	All	All
Hardware	Intel	Ethernet Connection X557	-	All	All	All

References

Reference	Source	Link	Tags
Intel SA-00555 Ethernet Controller Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
INTEL-SA-00555	MISC	www.intel.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161334 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2024-12110)

180432 Debian Security Update for linux (CVE-2021-33098)

390294 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2024-0002)

671367 EulerOS Security Update for kernel (EulerOS-SA-2022-1308)

671436 EulerOS Security Update for kernel (EulerOS-SA-2022-1352)

671448 EulerOS Security Update for kernel (EulerOS-SA-2022-1450)

671498 EulerOS Security Update for kernel (EulerOS-SA-2022-1466)

671535 EulerOS Security Update for kernel (EulerOS-SA-2022-1508)

671561 EulerOS Security Update for kernel (EulerOS-SA-2022-1523)

671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)

751590 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0056-1)

751600 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0068-1)

751602 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0080-1)

751654 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0197-1)

751695 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0367-1)

751697 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0366-1)

751698 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0362-1)

751701 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0366-1)

751702 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0371-1)

753133 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0181-1)

753264 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0079-1)

753355 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0056-1)

© 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 registred 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**