



CVE-2022-40233

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

Summary

CVE	CVE-2022-40233
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-23 19:15:00 UTC
Updated	2023-11-07 03:52:00 UTC
Description	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	ibm	Aix	7.1	All	All	All
Operating System	ibm	Aix	7.2	All	All	All
Operating System	ibm	Aix	7.3	All	All	All
Application	ibm	Vios	3.1	All	All	All

References

Reference	Source	Link	Tags
Security Bulletin: AIX is vulnerable to denial of service vulnerabilities	MISC	www.ibm.com	
IBM X-Force Exchange	MISC	exchange.xforce.ibmcloud.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

330115 IBM AIX Privilege Escalation Vulnerability (kernel_advisory5)

330118 IBM AIX Transmission Control Protocol/Internet Protocol (TCP/IP) Kernel Extension Denial of Service (DoS) Vulnerability (kernel_advisory5)

© [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](#)