



CVE-2023-28528

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-28528
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-28 03:15:00 UTC
Updated	2023-05-18 16:15:00 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 invscout command

Risk And Classification

Problem Types: CWE-78

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
IBM X-Force Exchange	MISC	exchange.xforce.ibmcloud.com
Security Bulletin: AIX is vulnerable to arbitrary command execution due to invscout (CVE-2023-28528)	MISC	www.ibm.com
IBM AIX 7.2 inscout Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[330134](#) IBM AIX Inventory Scout Arbitrary Command Execution Vulnerability (invscout_advisory4)

© [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](#)