

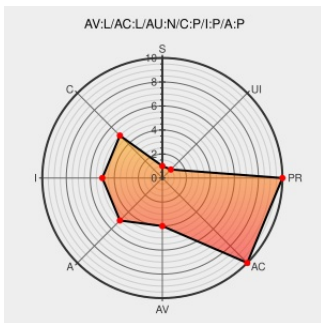


CVE-2005-2232

Published on: 07/12/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:27 PM UTC

CVE-2005-2232

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Aix](#) from [Ibm](#) contain the following vulnerability:

Buffer overflow in invscout in IBM AIX 5.1.0 through 5.3.0 might allow local users to execute arbitrary code via a long command line argument.

CVE-2005-2232 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM AIX Invscout Local Buffer Overflow Vulnerability

Exploit
Patch
cve.report (archive)
text/html

BID 13909

Exploit
Vendor Advisory
www.caughq.org
text/plain
Inactive Link Not Archived

MISC
www.caughq.org/advisories/CAU-2005-0002.txt

SecurityTracker.com Archives - IBM AIX Buffer Overflows in invscout, paginit, diagTasksWebSM, getluname, and swcons Commands and Multiple p Commands Let Local Users Execute Arbitrary Code

Exploit
securitytracker.com
text/html

SECTRAK 1014132

Secunia - Advisories - AIX Multiple Privilege Escalation

Exploit

SECUNIA 15636

Security Advisories: AIX Multiple Privilege Escalation Vulnerabilities

Exploit
Patch
Vendor Advisory
web.archive.org
text/html

CONFIRM

Malformed Request

Exploit
Vendor Advisory
www.securityfocus.com
text/html

CONFIRM
www.securityfocus.com/advisories/8816

Inactive Link Not Archived

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	ibm	Aix	5.1	All	All	All
Operating System	ibm	Aix	5.2	All	All	All
Operating System	ibm	Aix	5.3	All	All	All
Operating System	ibm	Aix	5.1	All	All	All
Operating System	ibm	Aix	5.2	All	All	All
Operating System	ibm	Aix	5.3	All	All	All
cpe:2.3:o:ibm:aix:5.1:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.2:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.3:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.1:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.2:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

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](#)