

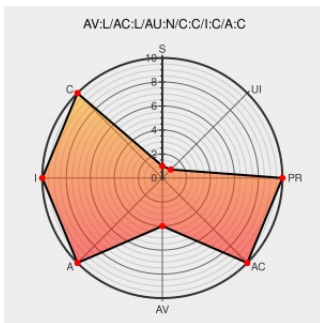


CVE-2004-1054

Published on: 12/22/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1054

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

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

Untrusted execution path vulnerability in invscout in IBM AIX 5.1.0, 5.2.0, and 5.3.0 allows local users to gain privileges by modifying the PATH environment variable to point to a malicious "uname" program, which is executed from lsvpd after lsvpd has been invoked by invscout.

CVE-2004-1054 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description	Tags	Link
Search results	www-1.ibm.com text/html	AIXAPAR IY64820
Search results	www-1.ibm.com text/html	AIXAPAR IY64852
iDEFENSE	Vendor Advisory www.idefense.com text/html	IDEFENSE 20041220 IBM AIX invscout Local Command Execution Vulnerability
Search results	www-1.ibm.com text/html	AIXAPAR IY64976
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF aix-invscout-gain-privileges(18619)

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	5.1l	All	All	All
Operating System	Ibm	Aix	5.2	All	All	All
Operating System	Ibm	Aix	5.2.2	All	All	All
Operating System	Ibm	Aix	5.2_l	All	All	All
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	5.3_l	All	All	All
Operating System	Ibm	Aix	5.1	All	All	All
Operating System	Ibm	Aix	5.1l	All	All	All
Operating System	Ibm	Aix	5.2	All	All	All
Operating System	Ibm	Aix	5.2.2	All	All	All
Operating System	Ibm	Aix	5.2_l	All	All	All
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	5.3_l	All	All	All
cpe:2.3:o:ibm:aix:5.1:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.1l:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.2:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.2.2:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:5.2_l:*:*:*:*:*:						

cpe:2.3:o:ibm:aix:5.3:*****:
cpe:2.3:o:ibm:aix:5.3_1:*****:
cpe:2.3:o:ibm:aix:5.1:*****:
cpe:2.3:o:ibm:aix:5.1l:*****:
cpe:2.3:o:ibm:aix:5.2:*****:
cpe:2.3:o:ibm:aix:5.2.2:*****:
cpe:2.3:o:ibm:aix:5.2_1:*****:
cpe:2.3:o:ibm:aix:5.3:*****:
cpe:2.3:o:ibm:aix:5.3_1:*****:

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](#)