

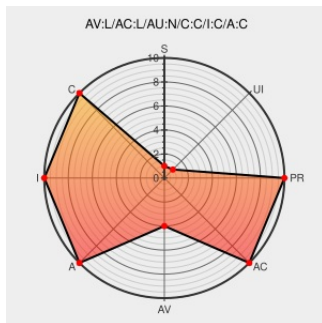


CVE-2004-1028

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

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1028

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

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

Untrusted execution path vulnerability in chcod on AIX IBM 5.1.0, 5.2.0, and 5.3.0 allows local users to execute arbitrary programs by modifying the PATH environment variable to point to a malicious "grep" program, which is executed from chcod.

CVE-2004-1028 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 IY64355](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF aix-chcod-gain-privileges\(18625\)](#)

iDEFENSE

[Vendor Advisory](#)
[www.iddefense.com](#)
[text/html](#)

[IDEFENSE 20041220 IBM AIX chcod Local Privilege Escalation Vulnerability](#)

Search results

[www-1.ibm.com](#)
[text/html](#)

[AIXAPAR IY64356](#)

Search results

[www-1.ibm.com](#)
[text/html](#)

[AIXAPAR IY64354](#)

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_:*****:
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_:*****:
cpe:2.3:o:ibm:aix:5.3:*****:
cpe:2.3:o:ibm:aix:5.3_:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)