



CVE-2004-2312

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2312

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

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

Buffer overflow in GNU make for IBM AIX 4.3.3, when installed setgid, allows local users to gain privileges via a long CC argument.

CVE-2004-2312 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

No Description Provided

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[FULLDISC 20040322 AIX 4.3.3 has make sgid 0?](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[text/html](#)

[XF aix-make-cc-bo\(15554\)](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 4391](#)

Inactive Link Not Archived

GNU Make For IBM AIX CC Path Local Buffer Overflow Vulnerability

[Exploit](#)

[cve.report \(archive\)](#)

[text/html](#)

[BID 9903](#)

Neohapsis Archives - Full Disclosure List - #1124 - Re: [Full-Disclosure] AIX 4.3.3 has make sgid 0?

[web.archive.org](#)

[text/html](#)

[FULLDISC 20040323 Re: AIX 4.3.3 has make sgid 0?](#)

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	4.3.3	All	All	All
Operating System	ibm	Aix	4.3.3	All	All	All
cpe:2.3:o:ibm:aix:4.3.3:*:*:*:*:*:						
cpe:2.3:o:ibm:aix:4.3.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→