

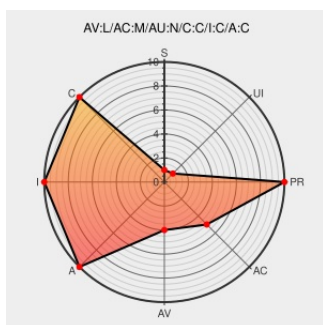


CVE-2012-2179

Published on: 06/22/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:27 PM UTC

CVE-2012-2179

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

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

libodm.a in IBM AIX 5.3, 6.1, and 7.1 allows local users to overwrite arbitrary files via a symlink attack on a temporary file.

CVE-2012-2179 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

[Patch](#)
[Vendor Advisory](#)
[aix.software.ibm.com](#)
[text/plain](#)

[CONFIRM](#)
[aix.software.ibm.com/aix/efixes/security/libodm_advisory.asc](#)

IBM IV21381: POTENTIAL SECURITY
ISSUE. APPLIES TO AIX 6100-07

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

[AIXAPAR IV21381](#)

IBM IV21383: POTENTIAL SECURITY
ISSUE. APPLIES TO AIX 7100-01

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

[AIXAPAR IV21383](#)

IBM IV22019: POTENTIAL SECURITY
ISSUE. APPLIES TO AIX 5300-12

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

[AIXAPAR IV22019](#)

IBM AIX Symlink Flaw in libodm Lets Local Users Gain Elevated Privileges - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

 SECTrack 1027193

IBM X-Force Exchange

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

 XF aix-libodm-symlink(75510)

No Description Provided

[www.osvdb.org](#)

Inactive LinkNot Archived

 OSVDB 83133

IBM IV21379: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 6100-06

Vendor Advisory

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

 AIXAPAR IV21379

IBM IV21382: POTENTIAL SECURITY ISSUE. APPLIES TO AIX 7100-00

Vendor Advisory

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

 AIXAPAR IV21382

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	5.3	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	7.1	All	All	All
Operating System	Ibm	Aix	5.3	All	All	All
Operating System	Ibm	Aix	6.1	All	All	All
Operating System	Ibm	Aix	7.1	All	All	All

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

cpe:2.3:o:ibm:aix:6.1:*:*:*:*:*:

cpe:2.3:o:ibm:aix:7.1:*:*:*:*:*:

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

cpe:2.3:o:ibm:aix:6.1:*:*:*:*:*:

cpe:2.3:o:ibm:aix:7.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2024   |

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](#)