

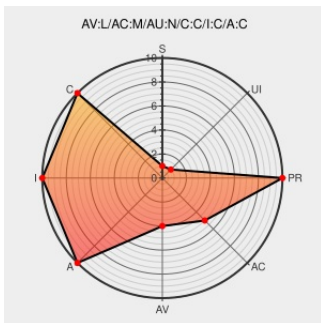


CVE-2014-3977

Published on: 06/08/2014 12:00:00 AM UTC

Last Modified on: 08/31/2021 03:44:00 PM UTC

CVE-2014-3977

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

Certain versions of [Aix](#) from [Ibm](#) contain the following vulnerability: libodm.a in IBM AIX 6.1 and 7.1, and VIOS 2.2.x, allows local users to overwrite arbitrary files via a symlink attack on a temporary file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-2179.

CVE-2014-3977 has been assigned by [M](#) cve@mitre.org 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

IBM AIX 6.1.8 libodm - Arbitrary File Write

www.exploit-db.com
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 33725](#)

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

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

IV60311: A POTENTIAL SECURITY ISSUE EXISTS CVE-2012-2179 APPLIES TO AIX 6100-08

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

[AIXAPAR IV60311](#)

IV60313: A POTENTIAL SECURITY ISSUE EXISTS CVE-2012-2179 APPLIES TO AIX 6100-07

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

[AIXAPAR IV60313](#)

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

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

[SECTRAK 1030401](#)

SecurityTracker		
CVE-2014-3977 - Portcullis	www.portcullis-security.com text/html	 MISC www.portcullis-security.com/security-research-and-downloads/security-advisories/cve-2014-3977/
IBM AIX 6.1.8+ Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/127067/IBM-AIX-6.1.8-Privilege-Escalation.html
IV60314: A POTENTIAL SECURITY ISSUE EXISTS CVE-2012-2179 APPLIES TO AIX 7100-02	www.ibm.com text/html	 AIXAPAR IV60314
IV60312: A POTENTIAL SECURITY ISSUE EXISTS CVE-2012-2179 APPLIES TO AIX 7100-01	www.ibm.com text/html	 AIXAPAR IV60312
IV60299: A POTENTIAL SECURITY ISSUE EXISTS CVE-2012-2179 APPLIES TO AIX 6100-09	www.ibm.com text/html	 AIXAPAR IV60299
IV60303: A POTENTIAL SECURITY ISSUE EXISTS CVE-2012-2179 APPLIES TO AIX 7100-03	www.ibm.com text/html	 AIXAPAR IV60303
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF aix-libodm-symlink(93595)

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	6.1	All	All	All
Operating System	ibm	Aix	7.1	All	All	All
Operating System	ibm	Aix	6.1	All	All	All
Operating System	ibm	Aix	7.1	All	All	All
Application	ibm	Vios	2.2.0.10	All	All	All
Application	ibm	Vios	2.2.0.11	All	All	All
Application	ibm	Vios	2.2.0.12	All	All	All
Application	ibm	Vios	2.2.0.13	All	All	All
Application	ibm	Vios	2.2.1.0	All	All	All
Application	ibm	Vios	2.2.1.1	All	All	All
Application	ibm	Vios	2.2.1.3	All	All	All
Application	ibm	Vios	2.2.1.4	All	All	All

Application	IBM	Vios	2.2.1.4	fp-25_sp-02	All	All
Application	lbm	Vios	2.2.1.4	fp-25_sp-02	All	All
Application	lbm	Vios	2.2.1.8	All	All	All
Application	lbm	Vios	2.2.1.9	All	All	All
Application	lbm	Vios	2.2.2.0	All	All	All
Application	lbm	Vios	2.2.2.4	All	All	All
Application	lbm	Vios	2.2.2.5	All	All	All
Application	lbm	Vios	2.2.3.0	All	All	All
Application	lbm	Vios	2.2.3.2	All	All	All
Application	lbm	Vios	2.2.3.3	All	All	All
Operating System	lbm	Vios	2.2.0.10	All	All	All
Operating System	lbm	Vios	2.2.0.11	All	All	All
Operating System	lbm	Vios	2.2.0.12	All	All	All
Operating System	lbm	Vios	2.2.0.13	All	All	All
Operating System	lbm	Vios	2.2.1.0	All	All	All
Operating System	lbm	Vios	2.2.1.1	All	All	All
Operating System	lbm	Vios	2.2.1.3	All	All	All
Operating System	lbm	Vios	2.2.1.4	All	All	All
Operating System	lbm	Vios	2.2.1.4	fp-25_sp-02	All	All
Operating System	lbm	Vios	2.2.1.8	All	All	All
Operating System	lbm	Vios	2.2.1.9	All	All	All
Operating System	lbm	Vios	2.2.2.0	All	All	All
Operating System	lbm	Vios	2.2.2.4	All	All	All
Operating System	lbm	Vios	2.2.2.5	All	All	All
Operating System	lbm	Vios	2.2.3.0	All	All	All
Operating System	lbm	Vios	2.2.3.2	All	All	All
Operating System	lbm	Vios	2.2.3.3	All	All	All

Operating System	ibm	Vios	2.2.0.10	All	All	All
Operating System	ibm	Vios	2.2.0.11	All	All	All
Operating System	ibm	Vios	2.2.0.12	All	All	All
Operating System	ibm	Vios	2.2.0.13	All	All	All
Operating System	ibm	Vios	2.2.1.0	All	All	All
Operating System	ibm	Vios	2.2.1.1	All	All	All
Operating System	ibm	Vios	2.2.1.3	All	All	All
Operating System	ibm	Vios	2.2.1.4	All	All	All
Operating System	ibm	Vios	2.2.1.4	fp-25_sp-02	All	All
Operating System	ibm	Vios	2.2.1.8	All	All	All
Operating System	ibm	Vios	2.2.1.9	All	All	All
Operating System	ibm	Vios	2.2.2.0	All	All	All
Operating System	ibm	Vios	2.2.2.4	All	All	All
Operating System	ibm	Vios	2.2.2.5	All	All	All
Operating System	ibm	Vios	2.2.3.0	All	All	All
Operating System	ibm	Vios	2.2.3.2	All	All	All
Operating System	ibm	Vios	2.2.3.3	All	All	All
cpe:2.3:o:ibm:aix:6.1:*****:						
cpe:2.3:o:ibm:aix:7.1:*****:						
cpe:2.3:o:ibm:aix:6.1:*****:						
cpe:2.3:o:ibm:aix:7.1:*****:						
cpe:2.3:a:ibm:vios:2.2.0.10:*****:						
cpe:2.3:a:ibm:vios:2.2.0.11:*****:						
cpe:2.3:a:ibm:vios:2.2.0.12:*****:						

cpe:2.3:a:ibm:vios:2.2.0.13:*****:
cpe:2.3:a:ibm:vios:2.2.1.0:*****:
cpe:2.3:a:ibm:vios:2.2.1.1:*****:
cpe:2.3:a:ibm:vios:2.2.1.3:*****:
cpe:2.3:a:ibm:vios:2.2.1.4:*****:
cpe:2.3:a:ibm:vios:2.2.1.4:fp-25_sp-02:*****:
cpe:2.3:a:ibm:vios:2.2.1.8:*****:
cpe:2.3:a:ibm:vios:2.2.1.9:*****:
cpe:2.3:a:ibm:vios:2.2.2.0:*****:
cpe:2.3:a:ibm:vios:2.2.2.4:*****:
cpe:2.3:a:ibm:vios:2.2.2.5:*****:
cpe:2.3:a:ibm:vios:2.2.3.0:*****:
cpe:2.3:a:ibm:vios:2.2.3.2:*****:
cpe:2.3:a:ibm:vios:2.2.3.3:*****:
cpe:2.3:o:ibm:vios:2.2.0.10:*****:
cpe:2.3:o:ibm:vios:2.2.0.11:*****:
cpe:2.3:o:ibm:vios:2.2.0.12:*****:
cpe:2.3:o:ibm:vios:2.2.0.13:*****:
cpe:2.3:o:ibm:vios:2.2.1.0:*****:
cpe:2.3:o:ibm:vios:2.2.1.1:*****:
cpe:2.3:o:ibm:vios:2.2.1.3:*****:
cpe:2.3:o:ibm:vios:2.2.1.4:*****:
cpe:2.3:o:ibm:vios:2.2.1.4:fp-25_sp-02:*****:
cpe:2.3:o:ibm:vios:2.2.1.8:*****:
cpe:2.3:o:ibm:vios:2.2.1.9:*****:
cpe:2.3:o:ibm:vios:2.2.2.0:*****:
cpe:2.3:o:ibm:vios:2.2.2.4:*****:
cpe:2.3:o:ibm:vios:2.2.2.5:*****:
cpe:2.3:o:ibm:vios:2.2.3.0:*****:

cpe:2.3:o:ibm:vios:2.2.0.0:*****:
cpe:2.3:o:ibm:vios:2.2.3.2:*****:
cpe:2.3:o:ibm:vios:2.2.3.3:*****:
cpe:2.3:o:ibm:vios:2.2.0.10:*****:
cpe:2.3:o:ibm:vios:2.2.0.11:*****:
cpe:2.3:o:ibm:vios:2.2.0.12:*****:
cpe:2.3:o:ibm:vios:2.2.0.13:*****:
cpe:2.3:o:ibm:vios:2.2.1.0:*****:
cpe:2.3:o:ibm:vios:2.2.1.1:*****:
cpe:2.3:o:ibm:vios:2.2.1.3:*****:
cpe:2.3:o:ibm:vios:2.2.1.4:*****:
cpe:2.3:o:ibm:vios:2.2.1.4:fp-25_sp-02:*****:
cpe:2.3:o:ibm:vios:2.2.1.8:*****:
cpe:2.3:o:ibm:vios:2.2.1.9:*****:
cpe:2.3:o:ibm:vios:2.2.2.0:*****:
cpe:2.3:o:ibm:vios:2.2.2.4:*****:
cpe:2.3:o:ibm:vios:2.2.2.5:*****:
cpe:2.3:o:ibm:vios:2.2.3.0:*****:
cpe:2.3:o:ibm:vios:2.2.3.2:*****:
cpe:2.3:o:ibm:vios:2.2.3.3:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)