



CVE-2014-8904

Published on: 01/15/2015 12:00:00 AM UTC

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

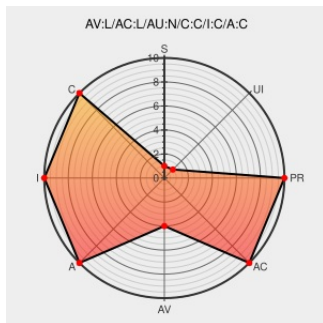
CVE-2014-8904

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

lquerylv in cmdlvm in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x allows local users to gain privileges via a crafted DBGCMD_LQUERYLV environment-variable value.

CVE-2014-8904 has been assigned by psirt@us.ibm.com 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

IBM X-Force Exchange

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

[XF ibm-aix-cve20148904-sec-bypass\(99193\)](#)

Security Advisory SA62195 - IBM AIX / Virtual
I/O Server lquerylv Privilege Escalation
Vulnerability - Secunia

[web.archive.org](https://web.archive.org/text/html)
text/html

[SECUNIA 62195](#)

Vendor Advisory
[aix.software.ibm.com](https://aix.software.ibm.com/text/plain)
text/plain

CONFIRM
aix.software.ibm.com/aix/efixes/security/lvm_advisory.asc

IBM AIX lquerylv Command Lets Local Users
Gain Root Privileges - SecurityTracker

[www.securitytracker.com](https://www.securitytracker.com/text/html)
text/html

[SECTrack 1031596](#)

IV67907: LQUERYLV SECURITY
VULNERABILITY (CVE-2014-8904) APPLIES
TO AIX 6100-09

[www.ibm.com](https://www.ibm.com/text/html)
text/html

[AIXAPAR IV67907](#)

IBM IV67908: LQUERYLV SECURITY VULNERABILITY (CVE-2014-8904) APPLIES TO AIX 7100-03	www.ibm.com text/html	 AIXAPAR IV67908
IBM IV68478: LQUERYLV SECURITY VULNERABILITY (CVE-2014-8904) APPLIES TO AIX 7100-02	www.ibm.com text/html	 AIXAPAR IV68478
IBM IV68082: LQUERYLV SECURITY VULNERABILITY (CVE-2014-8904) APPLIES TO AIX 6100-08	www.ibm.com text/html	 AIXAPAR IV68082
AIX 7.1 - 'lquerylv' Local Privilege Escalation - AIX local Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 38576
IBM IV68070: LQUERYLV SECURITY VULNERABILITY (CVE-2014-8904)	www.ibm.com text/html	 AIXAPAR IV68070
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
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	lbn	Vios	2.2.1.5	All	All	All
Application	lbn	Vios	2.2.1.6	All	All	All
Application	lbn	Vios	2.2.1.7	All	All	All
Application	lbn	Vios	2.2.1.8	All	All	All
Application	lbn	Vios	2.2.1.9	All	All	All
Application	lbn	Vios	2.2.2.0	All	All	All
Application	lbn	Vios	2.2.2.1	All	All	All
Application	lbn	Vios	2.2.2.2	All	All	All
Application	lbn	Vios	2.2.2.3	All	All	All
Application	lbn	Vios	2.2.2.4	All	All	All
Application	lbn	Vios	2.2.2.5	All	All	All
Application	lbn	Vios	2.2.3.0	All	All	All
Application	lbn	Vios	2.2.3.1	All	All	All
Application	lbn	Vios	2.2.3.2	All	All	All
Application	lbn	Vios	2.2.3.3	All	All	All
Application	lbn	Vios	2.2.3.4	All	All	All
Operating System	lbn	Vios	2.2.0.10	All	All	All
Operating System	lbn	Vios	2.2.0.11	All	All	All
Operating System	lbn	Vios	2.2.0.12	All	All	All
Operating System	lbn	Vios	2.2.0.13	All	All	All
Operating System	lbn	Vios	2.2.1.0	All	All	All
Operating System	lbn	Vios	2.2.1.1	All	All	All
Operating System	lbn	Vios	2.2.1.3	All	All	All
Operating System	lbn	Vios	2.2.1.4	All	All	All
Operating System	lbn	Vios	2.2.1.5	All	All	All
Operating System	lbn	Vios	2.2.1.6	All	All	All
Operating System	lbn	Vios	2.2.1.7	All	All	All
Operating System	lbn	Vios	2.2.1.8	All	All	All
Operating System	lbn	Vios	2.2.1.9	All	All	All

System						
Operating System	lbn	Vios	2.2.2.0	All	All	All
Operating System	lbn	Vios	2.2.2.1	All	All	All
Operating System	lbn	Vios	2.2.2.2	All	All	All
Operating System	lbn	Vios	2.2.2.3	All	All	All
Operating System	lbn	Vios	2.2.2.4	All	All	All
Operating System	lbn	Vios	2.2.2.5	All	All	All
Operating System	lbn	Vios	2.2.3.0	All	All	All
Operating System	lbn	Vios	2.2.3.1	All	All	All
Operating System	lbn	Vios	2.2.3.2	All	All	All
Operating System	lbn	Vios	2.2.3.3	All	All	All
Operating System	lbn	Vios	2.2.3.4	All	All	All
Operating System	lbn	Vios	2.2.0.10	All	All	All
Operating System	lbn	Vios	2.2.0.11	All	All	All
Operating System	lbn	Vios	2.2.0.12	All	All	All
Operating System	lbn	Vios	2.2.0.13	All	All	All
Operating System	lbn	Vios	2.2.1.0	All	All	All
Operating System	lbn	Vios	2.2.1.1	All	All	All
Operating System	lbn	Vios	2.2.1.3	All	All	All
Operating System	lbn	Vios	2.2.1.4	All	All	All
Operating System	lbn	Vios	2.2.1.5	All	All	All
Operating System	lbn	Vios	2.2.1.6	All	All	All
Operating System	lbn	Vios	2.2.1.7	All	All	All
Operating	lbn	Vios	2.2.1.8	All	All	All

System						
Operating System	lbn	Vios	2.2.1.9	All	All	All
Operating System	lbn	Vios	2.2.2.0	All	All	All
Operating System	lbn	Vios	2.2.2.1	All	All	All
Operating System	lbn	Vios	2.2.2.2	All	All	All
Operating System	lbn	Vios	2.2.2.3	All	All	All
Operating System	lbn	Vios	2.2.2.4	All	All	All
Operating System	lbn	Vios	2.2.2.5	All	All	All
Operating System	lbn	Vios	2.2.3.0	All	All	All
Operating System	lbn	Vios	2.2.3.1	All	All	All
Operating System	lbn	Vios	2.2.3.2	All	All	All
Operating System	lbn	Vios	2.2.3.3	All	All	All
Operating System	lbn	Vios	2.2.3.4	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:*****:						
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:2.2.1.5:*****:
cpe:2.3:a:ibm:vios:2.2.1.6:*****:
cpe:2.3:a:ibm:vios:2.2.1.7:*****:
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:2.2.2.1:*****:
cpe:2.3:a:ibm:vios:2.2.2.2:*****:
cpe:2.3:a:ibm:vios:2.2.2.3:*****:
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:2.2.3.1:*****:
cpe:2.3:a:ibm:vios:2.2.3.2:*****:
cpe:2.3:a:ibm:vios:2.2.3.3:*****:
cpe:2.3:a:ibm:vios:2.2.3.4:*****:
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:2.2.1.5:*****:
cpe:2.3:o:ibm:vios:2.2.1.6:*****:
cpe:2.3:o:ibm:vios:2.2.1.7:*****:
cpe:2.3:o:ibm:vios:2.2.1.8:*****:

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:2.2.2.1:*****:
cpe:2.3:o:ibm:vios:2.2.2.2:*****:
cpe:2.3:o:ibm:vios:2.2.2.3:*****:
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:2.2.3.1:*****:
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:2.2.3.4:*****:
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:2.2.1.5:*****:
cpe:2.3:o:ibm:vios:2.2.1.6:*****:
cpe:2.3:o:ibm:vios:2.2.1.7:*****:
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:2.2.2.1:*****:
cpe:2.3:o:ibm:vios:2.2.2.2:*****:

cpe:2.3:o:ibm:vios:2.2.2.3:*****:
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:2.2.3.1:*****:
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:2.2.3.4:*****:

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](#)