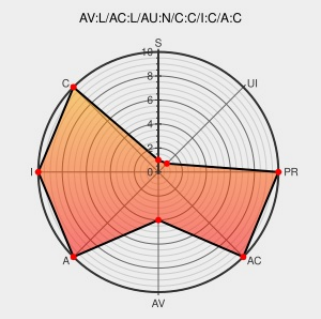
CVE-2004-1329

Published on: 12/20/2004 05:00:00 AM UTC

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

CVE-2004-1329

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Aix from Ibm contain the following vulnerability:

Untrusted execution path vulnerability in the diag commands (1) lsmcode, (2) diag_exec, (3) invscout, and (4) invscoutd in AIX 5.1 through 5.3 allows local users to execute arbitrary programs by modifying the DIAGNOSTICS environment variable to point to a malicious Dctrl program.

CVE-2004-1329 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070330 AIX 4.3 lsmcode local root command execution
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20070402 Re: AIX 4.3 lsmcode local root command execution
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF aix-diagnostics-gain-privileges(18620)
'AIX 5.1/5.2/5.3 local root exploits' - MARC	marc.info text/html	BUGTRAQ 20041220 AIX 5.1/5.2/5.3 local root exploits
AIX 4.3/5.1 - 5.3 lsmcode Local Root Command Execution	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 701
IBM AIX Diag Local Privilege Escalation	Exploit	BID 12041

Vulnerabilities	Patch Vendor Advisory cve.report (archive) text/html	
Search results	Patch Vendor Advisory www-1.ibm.com text/html	AIXAPAR IY64277
Search results	Patch Vendor Advisory www-1.ibm.com text/html	AIXAPAR IY64389

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_l:*:*:*:*:*:*:*
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_l:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→