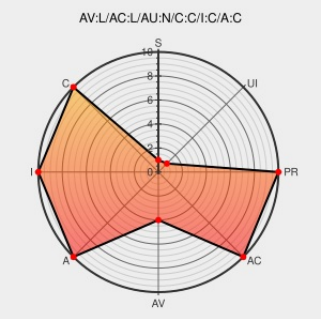
CVE-2005-2236

Published on: 07/12/2005 12:00:00 AM UTC

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

CVE-2005-2236

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



Certain versions of Aix from Ibm contain the following vulnerability:

Format string vulnerability in the paginit command in IBM AIX 5.3, and possibly other versions, might allow local users to execute arbitrary code via format strings in command line arguments.

CVE-2005-2236 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
IBM AIX PAGINIT Local Format String Vulnerability	Exploit, cve.report (archive), text/html	BID 13911
	Vendor Advisory, www.caughq.org, text/plain, Inactive Link, Not Archived	MISC www.caughq.org/advisories/CAU-2005-0003.txt
SecurityTracker.com Archives - IBM AIX Buffer Overflows in invscout, paginit, diagTasksWebSM, getlvname, and swcons Commands and Multiple p Commands Let Local Users Execute Arbitrary Code	securitytracker.com, text/html	SECTRACK 1014132

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	5.3	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→