CVE-2007-0670

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-0670
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-03 00:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Buffer overflow in bos.rte.libc in IBM AIX 5.2 and 5.3 allows local users to execute arbitrary code via the "r-commands", pos

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Ibm	Aix	5.2	All	All	All

Operating System	Ibm	Aix	5.3	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
IBM AIX Buffer Overflows in rsh, rcp, rlogin, and rdist Commands Let Local Users Gain Root Privileges - SecurityTracker	af854a3a-2127-42
IBM AIX RDist Unspecified Buffer Overflow Vulnerability	af854a3a-2127-42
IBM AIX Remote Access Commands Unspecified Buffer Overflow Vulnerability	af854a3a-2127-42
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-42
IBM X-Force Exchange	af854a3a-2127-42
aix.software.ibm.com/aix/efixes/security/README	af854a3a-2127-42
IBM notice: The page you requested cannot be displayed	af854a3a-2127-42
www.osvdb.org/31696	af854a3a-2127-42
IBM AIX Various R Commands Privilege Escalation Vulnerability - Advisories - Secunia	af854a3a-2127-42
IBM notice: The page you requested cannot be displayed	af854a3a-2127-42
SecurityTracker.com Archives - AIX Buffer Overflow in RDIST Command May Let Local Users Gain Elevated Privileges	af854a3a-2127-42
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.