



CVE-2007-3680

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

Summary

CVE	CVE-2007-3680
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-11 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Stack-based buffer overflow in the odm_searchpath function in libodm in IBM AIX 5.2.0 and 5.3.0 allows local users to exec

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Ibm	Aix	5.2.0	All	All	All

Operating System	ibm	Aix	5.3.0	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
SecurityTracker.com Archives - AIX Buffer Overflow in libodm May Let Local Users Gain Elevated Privileges				af854a3a-2127-422b-91ae-364		
labs.iddefense.com/intelligence/vulnerabilities/display.php				af854a3a-2127-422b-91ae-364		
IBM X-Force Exchange				af854a3a-2127-422b-91ae-364		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-2127-422b-91ae-364		
osvdb.org/36760				af854a3a-2127-422b-91ae-364		
aix.software.ibm.com/aix/efixes/security/README				af854a3a-2127-422b-91ae-364		
IBM notice: The page you requested cannot be displayed				af854a3a-2127-422b-91ae-364		
IBM AIX libodm ODMPATH Processing Buffer Overflow Vulnerability - Advisories - Secunia				af854a3a-2127-422b-91ae-364		
IBM AIX Libodm ODMPATH Stack Overflow Vulnerability				af854a3a-2127-422b-91ae-364		
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.						